Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)667 C

RECHTSWISSENSCHAFTLICHE FAKULTÄT
UNIVERSITÄT DES SAARLANDES

Lehrstuhl
für Rechtsinformatik

Prof. Dr. Christoph Sorge

Postfach 15 11 50
66041 Saarbrücken

Besucheranschrift:
Campus C3 1, Raum 1.25
66123 Saarbrücken

Tel. 0 681 / 302-51 22
Sekr. 0 681 / 302-51 20
E-Mail christoph.sorge@uni-saarland.de
Web www.legalinf.de

Saarbrücken, 10. Dezember 2020

Stellungnahme zum Entwurf eines Gesetzes zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze

Kernthesen

- Die Schaffung einer Verknüpfungsmöglichkeit zwischen Registern stellt einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung dar.
- Ein solcher Eingriff kann gerechtfertigt sein, aber jedenfalls nur, wenn ausreichende Schutzmaßnahmen vorgesehen sind.
- Der vorliegende Entwurf führt dazu, dass die Steuer-ID zu einem allgemeinen Personenkennzeichen wird. In der vorgesehenen Ausgestaltung ist ein solches allgemeines Personenkennzeichen verfassungswidrig.
- Die vorgesehenen Schutzmaßnahmen sind lückenhaft; die vorgesehenen Intermediäre können durch das Vorliegen eines allgemeinen Personenkennzeichens leichter umgangen werden, als dies nötig wäre.
- Die Einführung eines allgemeinen Personenkennzeichens ist schon deshalb nicht erforderlich, weil alternative Modelle mit bereichsspezifischen Personenkennzeichen existieren. In Österreich ist ein entsprechendes Modell etabliert. Angepasste Varianten sind auch in Deutschland, sogar auf Grundlage der durch den Entwurf des Registermodernisierungsgesetzes ohnehin vorgesehenen Struktur und mit überschaubarem Aufwand möglich.
- Auch ein System mit bereichsspezifischen Kennzeichen braucht zusätzliche rechtliche, technische und institutionelle Sicherungen, um datenschutzkonform umgesetzt werden zu können.
- Der vorliegende Entwurf läuft aufgrund dieser Bedenken Gefahr, durch das Bundesverfassungsgericht für nichtig erklärt zu werden. In diesem Fall würden sich Kosten- und Zeitaufwand bis zum Erreichen einer verfassungskonformen Lösung erheblich erhöhen.

A. Vorbemerkung

Die vorliegende Stellungnahme beruht – neben meiner eigenen Forschungserfahrung im Bereich des technischen Datenschutzes und angrenzender Rechtsfragen – wesentlich auf Erkenntnissen, die ich bei der Erstellung eines Gutachtens zu der Thematik gemeinsam mit Prof. Dr. rer. publ. Jörn von Lucke (Lehrstuhl für Verwaltungs- und Wirtschaftsinformatik, Zeppelin-Universität Friedrichshafen) und Prof. Dr. iur. Indra Spiecker gen. Döhmann (Lehrstuhl für Öffentliches Recht, Informationsrecht, Umweltrecht, Verwaltungswissenschaft, Goethe-Universität Frankfurt) gewonnen habe. Ich erlaube mir, an dieser Stelle lediglich einige der Kernaussagen wiederzugeben und für ausführliche Begründungen auf das Gutachten zu verweisen.

B. Einleitung

Der Wunsch nach einer verbesserten Datenqualität in staatlichen Registern ist nachvollziehbar. Falsche bzw. veraltete Daten können als Grundlage staatlicher Entscheidungen problematisch sein; schon ein Umzug, nach dem die Betroffenen nur noch mit erhöhtem Aufwand zu erreichen sind, erzeugt zusätzliche Kosten. Die Notwendigkeit, Daten zur Person bei den unterschiedlichsten Behörden immer wieder angeben zu müssen, kann zu Frustration bei den Betroffenen führen – wenngleich die meisten Bürger/innen nicht im ständigen Austausch mit Behörden stehen.

Eine Möglichkeit, Inkonsistenzen zu erkennen und Interaktionen mit der Verwaltung einfacher zu gestalten, liegt darin, Datenabrufe aus anderen Registern grundsätzlich möglich zu machen.

Diesen Erwägungen gegenüber steht die Feststellung, dass das Zusammenführen und der Abgleich von Daten aus verschiedenen Registern auch Grundlage für eine umfassende Profilbildung und Überwachung aller registrierten Personen sein kann: Sind Abrufe zur Erreichung legitimer Zwecke möglich, so gilt dies grundsätzlich auch für Abrufe zu illegitimen Zwecken. Schon die Schaffung einer Verknüpfungsmöglichkeit zwischen Registern stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar.

Technische und organisatorische Schutzmaßnahmen können dazu eingesetzt werden, diesen Risiken zu begegnen. Eine verfassungsgemäße Registermodernisierung, auch unter Schaffung (streng begrenzter) Datenübermittlungen zwischen Registern aus verschiedenen Verwaltungsbereichen, ist somit grundsätzlich möglich. Dem Entwurf des Registermodernisierungsgesetzes (RegMoG-E) ist dies jedoch nicht gelungen.

Diese Feststellung muss trotz einiger begrüßenswerter Ansätze und Sicherungsmechanismen getroffen werden, die im RegMoGE vorgesehen sind. Positiv hervorzuheben ist die Einführung eines Datencockpits, das Datenübermittlungen zwischen verschiedenen Registern und Behörden für die Betroffenen transparent machen soll.

Zum anderen ist ist auch die Einschaltung von Intermediären (Registermodernisierungsbehörde bzw. Vermittlungsstellen) eine sinnvolle Maßnahme, wenn auch nicht konsequent umgesetzt. Sofern Vermittlungsstellen eingesetzt werden, ist das 4-Corner-Modell vorgesehen. Im Kern wird dabei auf den Schutz durch einen „doppelten Umschlag“ gesetzt: Inhaltsdaten werden so verschlüsselt, dass die Intermediäre diese nicht lesen können. Lediglich Metadaten sind ihnen zugänglich. Auch diese Schutzmaßnahme ändert aber nichts an einem Grundproblem des Entwurfs.

C. Steuer-ID als allgemeines Personenkennzeichen

Dieses Problem besteht in der Weiterentwicklung der Steuer-ID zu einem allgemeinen Personenkennzeichen – wovon bei der zunächst vorgesehenen Verwendung in über 50 Registern unterschiedlichster Bereiche jedenfalls auszugehen ist. Verschärft wird dieses Problem bei einer späteren Ausdehnung auf zahlreiche weitere Register.

I. Risiken

Sieht man davon ab, dass das 4-Corner-Prinzip nicht für alle Datenübermittlungen vorgesehen ist, verbleibt ein offensichtliches Risiko: Die Steuer-ID als allgemeines Personenkennzeichen ermöglicht die Zuordnung von Daten auch unter Umgehung der Intermediäre. Zwar sind rechtliche Hürden eingerichtet; die Möglichkeit rechtswidrigen Handelns erscheint aber jedenfalls nicht fernliegend. Auch rechtmäßiges Zusammenführen von Daten konstituiert im Übrigen einen (wenn auch ggf. gerechtfertigten) Grundrechtseingriff.

Risiken entstehen nicht nur durch Verarbeitungsvorgänge öffentlicher Stellen. Steuer-IDs sind schon jetzt auch privaten Akteuren wie Arbeitgebern und Banken bekannt. Sollte das RegMoG-E in Kraft treten, ist ein adäquater Schutz der Steuer-ID kaum noch denkbar. Mit jeder Datenbank, in der Steuer-IDs gespeichert sind, steigt das Risiko erfolgreicher Cyberangriffe.

II. Verfassungswidrigkeit des vorgesehenen allgemeinen Personenkennzeichens

Für eine ausführliche Darstellung der verfassungsrechtlichen Problematik des vorgesehenen allgemeinen Personenkennzeichens wird auf das angehängte Gutachten verwiesen. Zusammenfassend lässt sich Folgendes feststellen:

- Der mit dem RegMoG-E zunächst angestrebte Zweck der Registermodernisierung ist legitim, wenn auch verfassungsrechtlich nicht von besonderem Gewicht. Für weitreichendere Ziele wie das „No-Stop-Government“ ist aber fraglich, ob diese überhaupt verfassungskonform umsetzbar sind.
- Die Einführung eines allgemeinen Personenkennzeichens ist für die Erreichung des angestrebten Ziels nicht erforderlich. Das gleiche Ziel lässt sich, mit geringerem Risiko, durch bereichsspezifische Kennzeichen erreichen. In Österreich ist ein entsprechendes System bereits etabliert. Das RegMoG-E geht in der Begründung zwar darauf ein, lehnt es jedoch aufgrund „größerer rechtlicher, technischer und organisatorischer Komplexität“ und dem außerordentlichen Kosten- und Zeitaufwand ohne weitere Nachweise ab. Während eine exakt identische Umsetzung tatsächlich problematisch sein könnte, lässt sich das Grundprinzip ohne weiteres übertragen. Wie bereichsspezifische Personenkennzeichen mit der Struktur des RegMoG-E in Einklang gebracht werden können, wird in Abschnitt D. skizziert.

- Das RegMoG-E betrifft einen außerordentlich großen Personenkreis. Gleichzeitig ist die Quantität der mit dem allgemeinen Personenkennzeichen verknüpften Daten schon nach dem jetzigen Stand sehr groß, mit der perspektivischen Ergänzung um weitere Register nahezu uferlos. Zugriffe auf diese Daten können zunächst ohne Kenntnis der Betroffenen erfolgen, auch wenn durch die Protokollierung und das Datencockpit eine nachträgliche Kontrolle möglich ist. Eine hinreichende Zweckbindung – die unter anderem auch ein Verbot der Verwendung des allgemeinen Personenkennzeichens durch Private beinhalten müsste – ist nicht vorgesehen. Der vorgesehene Missbrauchsschutz ist unzureichend, da unbestimmt. Bei der Bewertung der vorgesehenen Verknüpfungsmöglichkeiten ist auch die Gesamtbelastung der Bürger mit Informationseingriffen des Staates in den Blick zu nehmen. Es gilt zu verhindern, dass die gesamtheitliche Datenerfassung die Bürger dem Eindruck einer Totalüberwachung aussetzt. All dies führt dazu, dass die im RegMoG-E vorgesehenen Eingriffe selbst dann die Verhältnismäßigkeitsprüfung nicht bestehen, wenn man entgegen dem obigen Ergebnis davon ausgeht, die Einführung eines allgemeinen Personenkennzeichens sei für das angestrebte Ziel erforderlich.

Aufgrund der unzureichenden Konkretisierung gehen meine Co-Autoren und ich im Übrigen davon aus, dass auch die Verordnungsermächtigung des § 7 Abs. 2 S. 2 im Entwurf des Identifikationsnummerngesetzes (IDNrG-E) verfassungswidrig ist. Weder hat der Gesetzgeber vorgeben, welche Kriterien zur Bestimmung von Bereichen herangezogen werden sollen, noch hat er die Zahl bestimmt (lediglich die Untergrenze von sechs Bereichen ist benannt), noch hat er vorgegeben, welche Zielsetzung mit der Bereichsaufteilung einhergehen soll.

D. Alternativmodelle

Wie bereits ausgeführt, sind bereichsspezifische Personenkennzeichen im Vergleich zu allgemeinen Personenkennzeichen vorzugswürdig und ermöglichen eine verfassungskonforme Umsetzung der Registermodernisierung. Vergleichbar sind solche Kennzeichen etwa mit der heutigen Verwendung der Steuer-ID. Indem das RegMoG-E die Einführung verschiedener Verwaltungsbereiche vorsieht, liegt – trotz der unzureichenden Konkretisierung – bereits nahe, dass für diese Bereiche auch jeweils eigene Kennzeichen sinnvoll sind.

Auch die im RegMoG-E ebenfalls vorgesehenen Intermediäre erleichtern die Entwicklung alternativer Modelle für die Registermodernisierung. Zwei dieser Alternativen (Stammzahl-Modell nach österreichischem Vorbild und NEU-ID-Modell) sind im angehängten Gutachten dargestellt. Bei beiden werden bereichsspezifische Personenkennzeichen verwendet. Bereichsübergreifende Anfragen werden über die – im RegMoG-E ohnehin vorgesehenen – Intermediäre vermittelt, die aber die Zusatzfunktion erhalten, bereichsspezifische Kennzeichen zu „übersetzen“. Ein Intermediär bekommt also etwa eine Anfrage mit dem bereichsspezifischen Kennzeichen aus dem Bereich Meldewesen und leitet sie mit dem bereichsspezifischen Kennzeichen aus dem Bereich Steuern weiter. Bei der Weitervermittlung der Antwort wird der Vorgang in umgekehrter Richtung vorgenommen. Die Inhaltsdaten können, wie im RegMoG-E vorgesehen, weiterhin so verschlüsselt werden, dass der Intermediär auf diese nicht zugreifen kann.

Der im Vergleich zum RegMoG-E entstehende Mehraufwand betrifft im Wesentlichen nur die Intermediäre; auch dort ist er gering. Dass Intermediäre bereichsspezifische Kennzeichen einander

zuordnen können (und im Fall eines erfolgreichen Angriffs ggf. Dritte die gleiche Fähigkeit erhalten), ist keine Verschlechterung gegenüber dem durch das RegMoG-E vorgesehenen Modell. Wird ausschließlich die Steuer-ID verwendet, bestehen diese Zuordnungsmöglichkeiten ohnehin.

Dennoch ist auch in diesen Modellen mit bereichsspezifischen Kennzeichen ein zusätzlicher Missbrauchsschutz vorzusehen. Im o.g. Gutachten schlagen wir insbesondere die *institutionelle Unabhängigkeit der Intermediäre* vor. Diese könnten z.B. in Verantwortung der Datenschutzaufsichtsbehörden betrieben werden. Die Verteilung der Intermediärsrolle in einem *föderierten Ansatz*, etwa mit einem Intermediär pro Bundesland, ist mit etablierten technischen Verfahren möglich und kann Risiken weiter mindern. Auch plädieren wir für eine *Beschränkung der „Übersetzungsmöglichkeit"* der Intermediäre auf diejenigen bereichsspezifischen Kennzeichen, für die eine entsprechende *Notwendigkeit und Rechtsgrundlage* besteht; dies ist auch technisch abzusichern, beispielsweise durch *Hardware-Sicherheitsmodule*.

Mittelfristig sollte für geeignete Anwendungsfälle die Wahrnehmung der Intermediärs- und damit der „Übersetzungsfunktion" zwischen verschiedenen Bereichen auch beim jeweils Betroffenen, z.B. in einer App oder dem Personalausweis, angedacht werden.

E. Fazit

Gegen den vorliegenden Entwurf bestehen insgesamt also schwerwiegende Bedenken. Neben der grundsätzlichen Problematik, die durch die Schaffung einer Möglichkeit zum Zusammenführen von Daten aus zahlreichen Registern ergeben, ist auch die vorgesehene Umsetzung problematisch. Die Verfügbarkeit technischer Alternativen bei gleichzeitig hohem Missbrauchsrisiko wirkt sich auf die verfassungsrechtliche Bewertung aus. Ich halte es daher für riskant, das Gesetzgebungsverfahren fortzuführen und die Idee eines allgemeinen Personenkennzeichens weiter zu verfolgen. Die Gefahr, dass die vorgesehene Verwendung der Steuer-ID sich als verfassungswidrig herausstellt, ist groß. In diesem Fall dürften auch die sich ergebenden Kosten höher sein, als wenn bereits jetzt Alternativen entwickelt werden.

Gleichzeitig fügen sich die vorgeschlagenen Alternativmodelle so gut in die vorgesehene Struktur des RegMoG-E ein, dass einer zügigen Erarbeitung eines neuen Entwurfs nichts im Wege steht.

Saarbrücken, 10. Dezember 2020

Christoph Sorge

FRIEDRICH NAUMANN STIFTUNG Für die Freiheit.

REGISTER-MODERNISIERUNG

Datenschutzkonforme und umsetzbare Alternativen

Kurzanalyse zum Entwurf des Registermodernisierungsgesetzes

Christoph Sorge, Jörn von Lucke und Indra Spiecker gen. Döhmann

ANALYSE

Impressum

Herausgeber
Friedrich-Naumann-Stiftung für die Freiheit
Truman-Haus
Karl-Marx-Straße 2
14482 Potsdam-Babelsberg

/freiheit.org
/FriedrichNaumannStiftungFreiheit
/FNFreiheit

Autoren
Prof. Dr.-Ing. Christoph Sorge,
Lehrstuhl für Rechtsinformatik, Universität des Saarlandes

Prof. Dr. rer. publ. Jörn von Lucke,
Lehrstuhl für Verwaltungs- und Wirtschaftsinformatik,
Zeppelin Universität Friedrichshafen

Prof. Dr. iur. Indra Spiecker gen. Döhmann, LL.M. (Georgetown),
Lehrstuhl für Öffentliches Recht, Informationsrecht, Umweltrecht,
Verwaltungswissenschaften, Goethe-Universität Frankfurt

Redaktion
Dr. Maximilian Spohr
Liberales Institut
Friedrich-Naumann-Stiftung für die Freiheit

Produktion
COMDOK GmbH

Kontakt
Telefon +49 30 220126-34
Telefax +49 30 690881-02
E-Mail service@freiheit.org

Stand
Dezember 2020

Zentrale Aussagen und Empfehlungen

1. Der vorliegende Gesetzesentwurf zur Registermodernisierung (RegMoG-E) ist aus technischen und rechtlichen Gründen abzulehnen

2. Mit dem Entwurf ordnet die Regierung allen Bürger:innen in Gestalt der Steuer-ID ein **allgemeines Personenkennzeichen** zu, auch wenn zunächst nicht alle Register eingebunden werden.

3. Mittels eines solchen Systems können künftige Regierungen oder die Europäische Union erleichtert ein **Profil- und Überwachungssystem** über alle Bürger ausbauen.

4. Ein solches Gesetz wird mit hoher Wahrscheinlichkeit vor dem BVerfG scheitern

5. So droht in einigen Monaten ein Neustart des Vorhabens mit erheblichen Ver¬zögerungen und unnötigen Kosten.

6. Bundesregierung und der IT-Planungsrat müssen das laufende Gesetzgebungsverfahren stoppen!

7. Es gibt technisch und rechtliche besser Alternativen:

→ Alternative **„Stammzahl-Modell“**: orientiert sich am österreichischen Ansatz. Hier werden aus einer pro Person eindeutigen, geheim gehaltenen Stammzahl bereichsspezifische Kennzeichen mittels einer kryptographischen Hashfunktion abgeleitet. Intermediäre, die im RegMoG-E ohnehin vorgesehen sind, können diese Ableitung im Fall bereichsübergreifender Anfragen vornehmen. Die bereichsspezifischen Kennzeichen müssen allerdings sehr lang sein.

→ Alternative **„NEU-ID-Modell“**: es werden stattdessen bestehende oder zufällig generierte neue bereichsspezifische Kennzeichen verwendet. Auch hier erfolgt die Zuordnung dieser Kennzeichen durch ohnehin vorgesehene Intermediäre, die dafür entsprechende Zuordnungstabellen speichern müssen. Weitere personenbezogene Daten wie Namen oder Anschriften liegen ihnen nicht vor. Der Ansatz kommt mit kurzen, somit für Menschen gut handhabbaren bereichsspezifischen Kennzeichen aus.

→ Beide Ansätze müssen mit zusätzlichen Maßnahmen komplementiert werden: Dazu gehören die institutionelle Unabhängigkeit der Intermediäre und die Verteilung der Intermediärsrolle in einem föderierten Ansatz. Auch sollten Intermediäre möglichst nur diejenigen bereichsspezifischen Kennzeichen übersetzen können, für die eine entsprechende Notwendigkeit und Rechtsgrundlage besteht; dies ist auch technisch abzusichern, beispielsweise durch Hardware-Sicherheitsmodule. Mittelfristig sollte für geeignete Anwendungsfälle die Wahrnehmung der Intermediärs- und damit der Übersetzungsfunktion zwischen verschiedenen Bereichen auch beim Bürger, z.B. in einer App oder dem Personalausweis, angedacht werden.

→ Völlig risikofrei sind auch diese verbesserten Ansätze nicht – sie reduzieren aber die Risiken für den Datenschutz und die IT-Sicherheit, indem sie eine Umgehung der schon im Regierungsentwurf vorgesehenen Intermediäre erschweren.

8. Diese Alternativen könnten binnen weniger Monate und ohne nennenswerte Eingriffe in die bestehende Registerstruktur realisiert werden

Inhalt

A. Einführung

Mit dem Gesetzentwurf der Bundesregierung zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze, Registrierungsmodernisierungsgesetz (RegMoG-E)[1], plant das Bundesministerium des Innern, für Bau und Heimat (BMI) die Modernisierung der deutschen Verwaltungslandschaft durch die Einführung einer registerübergreifenden Identifikationsnummer. Zu diesem Zweck soll die bisher ausschließlich für Steuerverfahren genutzte Identifikationsnummer nach § 139b AO auf andere Bereiche erweitert werden. Alle anderen relevanten 56 registerführenden Stellen sollen innerhalb von fünf Jahren diese Identifikationsnummer als zusätzliches Ordnungsmerkmal zu Personendaten in ihren jeweiligen Registern speichern.

Bereits seit Bekanntwerden des Referentenentwurfs im Juli 2020 diskutiert die Öffentlichkeit über Sinn und Zweck einer solchen Kennziffer. Besondere Aufmerksamkeit erlangten die kritischen Stellungnahmen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)[2] und der Datenschutzkonferenz (DSK)[3]. Die erweiterte Verwendung der Identifikationsnummer ist vor dem Hintergrund, dass bereits bei Einführung vor deren schleichender Ausweitung gewarnt wurde,[4] als äußerst umstritten anzusehen.

I. Gesetzesentwurf der Bundesregierung

Bei dem RegMoG-E handelt es sich um ein Artikelgesetz, das mehrere Gesetze ändert beziehungsweise einführt. Von besonderer Bedeutung ist hierbei die Einführung des Identifikationsnummerngesetzes (IDNrG-E)[5]. Zu diesem Zweck wird die Verwendung der Steueridentifikationsnummer nach §§ 139a, b AO ausgeweitet.[6] Eine Identifikationsnummer wird nach dem Entwurf neben Steuerpflichtigen jeder natürlichen Person zugeordnet, die bei einer öffentlichen Stelle ein Verwaltungsverfahren führt (Art. 3 Nr. 1 RegMoG-E). Nach § 1 IDNrG-E wird diese Identifikationsnummer als zusätzliches Ordnungsmerkmal in 56 Register eingeführt, die in der Anlage zum IDNrG-E aufgelistet sind. Beispielhaft lassen sich hier Melderegister, Personenstandsregister und Ausländerzentralregister, aber auch Zentrales Fahrerlaubnisregister, Schuldnerverzeichnis und Beitragskontendatenbank nennen.

Für jede natürliche Person, die eine Identifikationsnummer erhalten hat, speichert das Bundeszentralamt für Steuern sogenannte Basis- und weitere Daten (§ 4 Abs. 1 IDNrG-E). Unter Basisdaten (§ 4 Abs. 2 IDNrG-E) versteht der Entwurf etwa Familienname, Vorname, Geburtsort und -datum, Geschlecht, Staatsangehörigkeit und andere. Weitere Daten (§ 4 Abs. 3 IDNrG-E) sind Auskunftssperren nach dem Bundesmeldegesetz, Datum des letzten Verwaltungskontakts (Monat und Jahr) und Validitätswerte (Hinweise zur Richtigkeit bestimmter Basisdaten, vgl. § 4 Abs. 5 IDNrG-E).

Zur Übermittlung dieser Daten sieht der Entwurf die Einrichtung einer Registermodernisierungsbehörde vor, die beim Bundesverwaltungsamt angesiedelt ist (§ 3 Abs. 1 S. 2 IDNrG-E). Sie dient als zwischengeschaltete Instanz zwischen den Behörden, die mittels der Identifikationsnummer auf Daten der Person zugreifen wollen. So können bei Übermittlung von mindestens Identifikationsnummer und Geburtsdatum alle Basis- und weitere Daten nach § 4 Abs. 2 und 3 IDNrG-E der Person an die abrufende Behörde übermittelt werden, soweit die Daten zur Aufgabenerfüllung erforderlich sind (§ 6 Abs. 3 Nr. 2 IDNrG-E). Umgekehrt kann bei Angabe von mindestens Familiennamen, Wohnort, Postleitzahl und Geburtsdatum die Identifikationsnummer ermittelt werden (§ 6 Abs. 3 Nr. 1 IDNrG-E). Nach Übermittlung der angeforderten Daten muss die Registermodernisierungsbehörde diese löschen (§ 11 IDNrG-E).

Ferner sieht Art. 2 RegMoG-E die Einführung eines sogenannten Datencockpits im Rahmen einer Modifizierung des Onlinezugangsgesetzes (OZG) vor. In diesem Datencockpit kann eine natürliche Person Auskunft zu Datenübermittlungen unter Rückgriff auf die Identifikationsnummer erhalten (§ 10 Abs. 1 OZG). Das Datencockpit zeigt lediglich Protokolldaten an (§ 10 Abs. 2 OZG), auf die nur die betroffene Person Zugriff hat (§ 4 Abs. 4 OZG). Diese Protokolldaten erheben die jeweiligen Stellen bei allen Datenübermittlungen unter Nutzung einer Identifikationsnummer (§ 9 Abs. 1 S. 1 IDNrG-E). Die Registermodernisierungsbehörde protokolliert darüber hinaus alle Datenübermittlungen von und zur Registermodernisierungsbehörde selbst (§ 9 Abs. 1 S. 2 IDNrG-E). Neben der Übermittlung an das Datencockpit dürfen diese Protokolldaten nur zur datenschutzrechtlichen Prüfung und zur Wahrnehmung von Betroffenenrechten verwendet werden (§ 9 Abs. 2 IDNrG-E). Nach zwei Jahren sind die Protokolldaten – vorbehaltlich zu begründender Ausnahmen – zu löschen (§ 9 Abs. 3 IDNrG-E).

Die verbleibenden Artikel des RegMoG-E beziehen sich auf Änderungen von Gesetzen zu Fachregistern, in denen zukünftig auch die übergreifende Identifikationsnummer gespeichert werden soll.[7]

[1] RegMoG-E: Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung, Bundestagsdrucksache 19-24226, Deutscher Bundestag, Berlin 2020. Online: https://dip21.bundestag.de/dip21/btd/19/242/1924226.pdf.
[2] *BfDI 2020*, Hintergrundpapier zur Registermodernisierung und Schaffung eines einheitlichen Personenkennzeichens [BfDI 2020].
[3] DSK 2020, Entschließung vom 26.08.2020, Registermodernisierung verfassungskonform umsetzen.
[4] Vgl. *BfDI 2010*, 23. Tätigkeitsbericht (2009/2010), S. 106.
[5] Art. 1 RegMoG-E: Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung.
[6] Vgl. zur Vergabe der Identifikationsnummer auch den Verweis des § 5 Abs. 2 IDNrG-E auf § 139b AO iVm. der Steueridentifikationsnummernverordnung.
[7] *Wissenschaftlicher Dienst des Deutschen Bundestages 2020,* Gutachten Einführung einer registerübergreifenden einheitlichen Identifikationsnummer nach dem Entwurf eines Registermodernisierungsgesetzes, S. 5 [Wiss. Dienst BTag, Gutachten].

II. Anforderungen an eine zeitgemäße Registermodernisierung

Zum eigentlichen Zweck der Registermodernisierung bei Bund, Ländern und Kommunen hat sich das Koordinierungsprojekt Registermodernisierung des IT-Planungsrats im April 2020 in einem Eckpunktepapier[8] geäußert. Diese abgestimmten Ergebnisse wurden in der 32. Sitzung des IT-Planungsrats vom 24. Juni 2020 von diesem zur Kenntnis genommen und bilden damit die Grundlage für die bis Ende 2020 anzufertigende Gesamtkonzeption für eine modernisierte Registerlandschaft. Im Kern geht es um den Aufbau eines registerübergreifenden Identitäts- und Qualitätsmanagements, um einen einfachen Datenaustausch zwischen allen beteiligten Stellen, um eine verbesserte Datenhaltung in Registern und elektronisch geführten Datenbeständen, um einen verbesserten Datenschutz, verbesserte Datensicherheit und Transparenz der Zugriffe sowie perspektivisch um eine Erweiterung der Registerlandschaft, um alle benötigten Daten vorzuhalten.

Das RegMoG-E der Bundesregierung, welches das Konzept des IT-Planungsrats aufgreift, ist ein zentrales Element für diese verwaltungsebenenübergreifende Modernisierung, die auch der Nationale Normenkontrollrat seit 2017 fordert.[9] Erstens soll nach Vorstellungen des IT-Planungsrats das registerübergreifende Identitäts- und Qualitätsmanagement künftig die Qualitätssicherung bestehender Datenbestände übernehmen und so zu einer inhaltlich optimalen Aufstellung beitragen. Dabei gilt es vor allem, Inkonsistenzen zu erkennen, Dubletten und Schreibfehler zu beseitigen sowie Namen und Adressen auf den aktuellen Stand zu bringen. Dies hat Korrekturen in allen beteiligten Registern zur Folge und kann über gemeinsame Basisdaten einfach realisiert werden. Zugleich soll eine Anbindung an föderale Integrationsbemühungen seitens der Europäischen Union vorbereitet werden.[10] Zweitens soll mit einem Architekturmodell, dem Ausbau von Standards und Schnittstellen, einer Anpassung der Transportwege und einer Erweiterung des Zugriffs- und Rechtemanagements auf neuer rechtlicher Grundlage der Datenaustausch zwischen allen zu beteiligenden Stellen verbessert werden.[11] Drittens gilt es alle datenhaltenden Behörden digital zu ertüchtigen, um mit gezielten Vollständigkeits-, Qualitäts- und Datensparsamkeitsmaßnahmen eine Verbesserung der Datenhaltung in der Bundesrepublik insgesamt zu erreichen. So werden die Etablierung eines Unternehmensregisters, eines Gebäude- und Wohnungsregisters und eines statistischen Bildungsregisters angedacht.[12] Ab 2030 wird ein künftig jährlicher registerbasierter Zensus (Volkszählung) in Erwägung gezogen.[13] Da dies alles zu einem „gläsernen Bürger" führen kann, sollen viertens weitere Datenschutz- und Sicherheitsmaßnahmen vor einer staatlichen Profilbildung sowie ein Datencockpit für mehr Transparenz des Bürgers über behördliche Zugriffe auf seine Daten etabliert werden.[14] Welche konkreten Vorstellungen allerdings diesem letzten Punkt Rechnung tragen sollen und wie eine (Selbst-)Kontrolle des Staates unter diesen Bedingungen gelingen soll, bleibt weitgehend offen.

Begründet durch den hohen gesellschaftlichen Stellenwert, der dem Datenschutz in Deutschland beigemessen wird sowie einer Tradition papierbasierter Aktenführung ist in der Bundesrepublik Deutschland auf staatlicher Ebene kaum ersichtlich, welche Daten die einzelnen Behörden von Bund, Land und Kommunen insgesamt über ihre Bürger vorhalten. Deutsche Behörden sind verpflichtet, die von ihnen erhobenen Daten nur für die gesetzlich definierten Zwecke zu verwenden. Die Erstellung von Persönlichkeitsprofilen der Bürger durch eine Zusammenführung der vorhandenen Lebens-, Verhaltens- und Personaldaten ist staatlichen Stellen untersagt. Dies leitet sich aus dem deutschen Grundgesetz ab und gilt auch auf europäischer Ebene. Darüber hinaus sind diese Grundsätze auch der Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshofs zu entnehmen.[15]

Im Vergleich zu vielen anderen europäischen Staaten ist Deutschland beim E-Government weder Vorreiter noch Treiber der technischen Entwicklung. Auf Grund des föderalen Mehrebenensystems dauert jede Umsetzung verwaltungsebenenübergreifender Modernisierungsansätze typischerweise länger. Durch Kompromisse ist sie wegen der unterschiedlichen Vorstellungen im Wettbewerb der politischen Ideen aber auch ausgewogener. Elektronische Register und die elektronische Akten- und Vorgangsbearbeitung lösen in den kommenden Jahren die letzten Bücher und Papierakten ab. Mit dem OZG und dem RegMoG wollen sich Bund, Länder und Kommunen für die digitale Zukunft leistungsfähig und bürgernah aufstellen.

Vor diesem Hintergrund erzeugt der von der Bundesregierung eingebrachte RegMoG-E erhebliche Irritationen. Mit einem allgemeinen Personenkennzeichen, das zunächst auf 57 Register – perspektivisch sogar auf alle derzeit bestehenden 220 und alle zukünftig zu entwickelnden Register (zum Beispiel das Register des Forschungsdatenzentrums mit den Versicherungsdaten aller gesetzlich Krankenversicherten nach § 303d DVG) ausgeweitet werden soll und kann –, wird (bewusst oder unbewusst) eine wesentliche Grundlage für die mögliche Generierung von Persönlichkeitsprofilen aller Bürger quer über die gesamte Verwaltung gelegt. Mit einer weiteren Gesetzesänderung und neuartigen Profilbildungsprogrammen könnten künftige Machthaber plötzlich und rasch wissen, was der Staat wirklich weiß und dies für oder gegen die Bürger einsetzen. Danach wäre aber technisch durchaus

[8] *IT-Planungsrat* 2020, Eckpunkte für die Registermodernisierung – Bestehende Anforderungen, vorläufige Architekturskizze sowie sich daraus ergebende Maßnahmen im Rahmen des IT-Planungsratsprojekts Registermodernisierung.
[9] Vgl. *Nationaler Normenkontrollrat 2017,* Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren.
[10] Vgl. *IT-Planungsrat* 2020, S. 3, S. 17 und S. 34.
[11] Vgl. *IT-Planungsrat* 2020, S. 4 und S. 18.
[12] Vgl. *IT-Planungsrat* 2020, S. 4 und S. 19.
[13] Vgl. *Nationaler Normenkontrollrat/McKinsey & Company* 2017, S. 21-23 und Körner/Krau¬se/Ram-sauer 2019.
[14] Vgl. *IT-Planungsrat* 2020, S. 2-3, S. 17-20 und S. 33-35.
[15] BVerfG 1 BvR 16/13 Rn. 90 ff. und EuGH ECLI:EU:C:2020:790 Rn.71 ff.

realisierbar, was nach geltendem Recht unzulässig ist und im Gesetzesentwurf zu Recht unter Strafe gestellt wird. Gerade deswegen stellt sich mit dem Gesetzesentwurf auch die Frage an den Gesetzgeber, ob der Staat in die Lage versetzt werden soll, auf Knopfdruck alles über seine Bevölkerung wissen zu können.

Der Datenschutz verfolgt ganz andere, höhere Ziele. Datenschutz besitzt für die Bundesrepublik Deutschland und ihre Bürger eine hohe Bedeutung. Dieser Stellenwert speist sich aus den Erfahrungen des Dritten Reiches, der Diktatur des Nationalsozialismus und der Deutschen Demokratischen Republik. Bürger wurden damals erfasst, überwacht, selektiert, verhaftet und ermordet. Dies darf sich niemals wieder wiederholen. Die Ermöglichung freiheitlichen Handelns durch den Datenschutz und IT-Sicherheit und damit ihre Funktion als Rückgrat von Demokratie, Grundrechtsverwirklichung und gleichen Verwirklichungschancen der Bürger ist vor diesem Hintergrund nicht zu unterschätzen.

Die Bundesrepublik ist von einem föderalen Mehrebenensystem geprägt, in dem es bis zu sieben Ebenen, mehr als 11.000 Gebietskörperschaften und mehr als 30.000 zuständige Ämter und Behörden gibt, die öffentliche Aufgaben wahrnehmen und gemeinsam über 5.900 Verwaltungsleistungen erbringen. Diese Komplexität der Aufbau- und Ablauforganisation ist für Bürger wie Verwaltung herausfordernd, aber politisch auch so gewollt. Mit dem Onlinezugangsgesetz soll Bürgern und Unternehmen nun der Zugang zu Verwaltungs-leistungen bis 2022 flächendeckend digital ermöglicht werden. Der Normenkontrollrat und die Bundesregierung erachten dazu auch eine Registermodernisierung als dringend erforderlich. Die wahrnehmbare Trennung der verschiedenen Ebenen wird damit reduziert.

In einer offenen Gesellschaft sollen zugleich alle Bürger die Freiheit haben, zu sein und zu agieren, wie sie sind und sein möchten. Der Staat darf deswegen nicht in die Lage versetzt werden, über umfassende Aktivitätsprofile aller seiner Einwohner zu verfügen, um diese zu einem (politisch) konformen Verhalten zu bewegen. Die zunehmende smarte, KI-basierte und plattformbasierte Überwachung im öffentlichen wie im privaten Raum eröffnet hier allen evidenzbasierten, verhaltenswissenschaftlichen Ansätzen in Echtzeit neuartige Möglichkeiten, die von Vertretern der Zivilgesellschaft und vieler Parteien zunehmend mit Sorge betrachtet werden. Vertreter vieler Sicherheitsbehörden haben dazu eine berufsbedingte, nachvollziehbar andere Einschätzung. Diese Behörden profitieren von umfassenden Profilen der gesamten Bevölkerung, etwa um mit Hilfe leistungsstarker IT-basierter Polizeianalysedienste präventiv potenzielle Gefährder frühzeitig zu identifizieren oder um nach Anschlägen rasch verfassungsfeindliche Netzwerke zu enttarnen und zu verhaften. Eine Zusammenarbeit mit zahlreichen Plattformen wäre für die Sicherheitsbehörden eine weitere, bereichernde Option.

Je nach Gefährdungslage kommen Entscheider im politischen Raum also zu unterschiedlichen Einschätzungen, wie staatliche Behörden mit den personenbezogenen Daten jetzt und in Zukunft umgehen sollen. Mit der Einführung einer Identifikationsnummer als allgemeines Personenkennzeichen würde in der Bundesrepublik Deutschland die Grundlage gelegt, dass die vorhandenen bereichsspezifischen Profile zu einem Bürger rasch zu einem umfassenden Gesamtprofil zusammen¬gefügt werden könnten. Die Bundesregierung sieht diese Gefahr durchaus. Sie schlägt mit dem Gesetzesentwurf einige organisatorische und strafrechtliche Maßnahmen vor, die dies dauerhaft unterbinden sollen. Darüber würde sich aber eine künftig gewählte, überwachungs- und selektionsfreudige Bundesregierung mit einer simplen wie gezielten Gesetzesänderung hinwegsetzen können. Die neu geschaffene Möglichkeit der Zusammenführung von Registerdaten durch ein allgemeines Personenkennzeichen ermöglicht zudem schon sofort eine – wenn auch rechtswidrige – Zusammenführung von Daten aus verschiedenen Registern unter Umgehung vorgesehener Schutzmechanismen. Die Bevölkerung müsste mit diesen Risiken und Nebenwirkungen dauerhaft leben. Dies ist aus verschiedenen Gründen inakzeptabel.

Das Ziel eines freiheitsermöglichenden Staates und einer gelebten offenen Gesellschaft muss dauerhaft der transparente Staat, nicht aber der „gläserne Bürger" sein. Die Bürger sollen verstehen können, wie der Staat funktioniert, welche Behörde welche Aufgaben erledigt und gegen wen bzw. gegen was sich effektiver Rechtsschutz zur Kontrolle richten kann. Diesem Auftrag widmet sich unter anderem das OZG. Die Behörden müssen die öffentlichen Aufgaben, die ihnen die Gesetzgeber übertragen, auch erfüllen können. Dazu benötigen sie Haushaltsmittel, Stellen, qualifiziertes Personal und organisatorische Prozesse, aber auch gewisse personenbezogene Daten der Bürger, die sie datenschutzkonform und zweckgerichtet zu verwenden und zur Erfüllung ihrer Zwecke sicher zu bewahren haben. Soweit dies zur öffentlichen Aufgabenerfüllung erforderlich ist, sollte jede Behörde in der Lage sein, bei Bedarf einen Ausschnitt eines Bildes aus dem Leben des Bürgers auf Basis der vorliegenden Daten in dem jeweiligen Amt oder Bereich zu generieren.

Trotz zunehmender Gesamtüberwachung und weitreichender Ausforschungsmöglichkeiten darf ein „gläserner Bürger" aber nicht Realität werden, denn dieser würde weder seine Kontrollfunktion noch seine Freiheitsdimension ausleben können. Daher dürfen der Staat und die Verwaltung nicht durch Informationstechnologien in die Lage versetzt werden, auf Knopfdruck zu einem Bürger ein umfassendes, detailliertes Profil auf Basis aller oder vieler vorliegender Datenbestände in den vorhandenen Registern von Bund, Ländern und Kommunen zu erstellen. Ebenso sollten sie kein neuartiges umfassendes Register mit allen Daten selbst erzeugen können.

Diese Gefahr würde nun mit dem Gesetzesentwurf zur Registermodernisierung und der Einführung einer Identifikationsnummer als einer allgemeinen, registerübergreifenden und zentralen Personenkennziffer, wie dort vorgesehen, ohne weitere Sicherungen deutlich gesteigert. Verfassungs- und europarechtlich ist dies nicht zulässig, wie in Teil B gezeigt wird.

III. Optionen für Personenkennzeichen

Die Bundesrepublik Deutschland und ihre Gesetzgeber haben sich bisher, auch basierend auf den erlebten Erfahrungen der Jahre 1933–1945 (nationalsozialistische Diktatur des Dritten Reiches), insbesondere mit Blick auf die Reduzierung von Häftlingen auf eine Nummer, sowie der Erfahrungen der Jahre 1949–1989 (kommunistische Diktatur der DDR), klar gegen allgemeine Personenkennzeichen ausgesprochen. Bisherige Versuche einzelner Fraktionen, ein allgemeines Personenkennzeichen einzuführen, scheiterten.

In vielen anderen europäischen und außereuropäischen Staaten wurden die Stärken und Schwächen sowie Chancen und Risiken dieses Ansatzes jedoch anders bewertet. Diese Staaten haben eine allgemeine Personenkennziffer oder ein Personenkennzeichen eingeführt, die Bürger ihr Leben lang im Kontakt mit Behörden und staatlichen Stellen verwenden. Auch Unternehmen nutzen seit vielen Jahrzehnten Kundennummern, damit sie im Bedarfsfall alle Daten zu einer Person (Kunde) rasch zuordnen können. In den Mitgliedstaaten der Europäischen Union werden verschiedene Konzepte verfolgt.[16]

Auch die Bundesrepublik Deutschland hat sich, in Anerkennung ihrer Geschichte, zur Vereinfachung von Verwaltungsvorgängen Personenkennzeichen bedient. Diese sind allerdings bereichsspezifisch ausgerichtet. Die Steuer-ID, die Renten¬versicherungsnummer, die Krankenversicherungsnummer und die Personenkennziffer der Bundeswehr sind Beispiele für bekannte bereichsspezifische Kennzeichen. Sie dürfen allerdings nur in einem bestimmten Verwaltungs- und Lebensbereich für bestimmte Aufgaben eingesetzt werden und erlauben keine weitere, gar flächendeckende Verwendung in anderen Lebens- und Verwaltungsbereichen.

Personenkennzeichen sind alphanumerische Zeichenfolgen, die zur eindeutigen Identifizierung von Personen innerhalb einer größeren Personengruppe dienen sollen. Aus dem Blickwinkel der Verwaltungsinformatik und der Verwaltungswissenschaft bestehen zahlreiche Optionen zur Gestaltung von Personenkennzeichen. Diese Optionen und Alternativen lassen sich in einem morphologischen Kasten (**Abbildung 1**) darstellen.

Abb. 1 | Morphologischer Kasten zu Personenkennzeichen

PK / ID-NR	AUSPRÄGUNGSFORMEN				
Einzigartigkeit	einzigartig			mehrfach vergeben	
Sichtbarkeit	nicht-sprechend			sprechend	
Ziffern oder Zeichen und Umfang des Zeichensatzes	numerische Ziffernreihenfolge (0-9)			alphanumerische Zeichenreihenfolge (0-9, A-Z, a-z)	
Prüfziffer	mit Prüfziffer			ohne Prüfziffer	
Typus von Personenkennzeichen	allgemeine Verwendung (aPK: wesentliche Bereiche)		bereichsübergreifende Verwendung (2wPK: 2 oder wenige Bereiche)		bereichsspezifische Verwendung (bPK: 1 Bereich)
Vorgehen bei der Vergabe	zentrale Vergabe			dezentrale Vergabe	
Zu erfassende Personengruppe	Deutsche Bürger	Ausländer	Steuerzahler	Natürliche Personen	Juristische Personen
Basisdatensatz	mit Basisdatensatz			ohne Basisdatensatz	

In der Regel sollten Personenkennzeichen einzigartig sein, damit sie Personen eindeutig identifizieren. Eine mehrfache Vergabe eines Personenkennzeichens mag sich als sinnvoll erweisen, etwa wenn der vorherige Träger des Kennzeichens verstorben und das Reservoir verfügbarer Ziffern oder Zeichenkombinationen erschöpft ist. Ein solches Vorgehen würde jedoch dem eigentlichen Zweck des Kennzeichens für Personen widersprechen und muss wegen des Risikos von Fehlzuordnungen schon prinzipiell verworfen werden.

Personenkennzeichen könnten sprechend angelegt sein. Dann lassen sich bestimmte Daten direkt aus dem Kennzeichen ablesen, etwa bei der Personenkennziffer der Bundeswehr das Geburtsdatum, der erste Buchstabe des Nachnamens und der Meldebezirk (früher das zuständige Kreiswehrersatzamt). Nicht-sprechende Personenkennzeichen verhindern diese Sichtbarkeit prinzipiell und machen die Person hinter dem Kennzeichen für Dritte nicht gläsern.

[16] Vgl. *Hansen, in: Simitis/Hornung/Spiecker gen. Döhmann* 2019, Art. 87 Rn. 31f.

Kennzeichen können aus einer rein numerischen Ziffernreihenfolge oder aus einer alphanumerischen Zeichenreihenfolge bestehen. Bei einer Nummer wird deswegen von einer Personenkennziffer, bei einem Zeichencode von einem Personenkennzeichen gesprochen. Je länger die Personenkennziffer oder das Personenkennzeichen ist, desto größer ist das Reservoir an verfügbaren Zeichenkombinationen. Bei einer numerischen Ziffernreihenfolge gibt es bis zu 10 Möglichkeiten (0-9), bei einer alphanumerischen Zeichenreihenfolge bestehen bis zu 62 Optionen (0-9 & A-Z & a-z) pro Zeichenposition. Eine Mischung von Groß- und Kleinschreibung wäre in der praktischen Umsetzung allerdings fehleranfällig. 36 Optionen (0-9 & A-Z) sind auch gut handhabbar. Sollen mindestens 84 Millionen Bundesbürger erfasst werden, bedarf eine numerische Personenkennziffer in der Bundesrepublik zumindest 9 numerischer Zeichen, ein alphanumerisches Personenkennzeichen zumindest 5 alphanumerischer Zeichen.

Prüfziffern in Personenkennzeichen dienen dazu, Fehler bei der manuellen Eingabe oder Datenübermittlung zu erkennen. Nach einem vereinbarten Algorithmus werden dazu die Ziffern oder Zeichen verrechnet. Das Ergebnis entspricht der Prüfziffer, die dem restlichen Kennzeichen angehängt oder vorangestellt wird und in der Praxis als Teil des Kennzeichens betrachtet wird. Zahlendreher und andere Fehleingaben generieren dagegen eine andere Prüfziffer, so dass Nutzer bei Fehleingaben zeitnah auf ihre Fehler hingewiesen werden können.

Ein allgemeines Personenkennzeichen (aPK) wird innerhalb eines Staates von allen Behörden, von vielen Behörden oder den wesentlichen Behörden verwendet, um Personen eindeutig zu identifizieren. Entscheidend ist dabei nicht die allein Anzahl der Behörden (im Vergleich zur Gesamtzahl aller Behörden), sondern die Breite der abgedeckten Lebensbereiche, in denen die Kennziffer verwendet wird. aPK werden in der Regel zentral vergeben, um sicherzustellen, dass jede Person auch nur ein einziges Mal erfasst und jede Personenkennziffer nur ein einziges Mal vergeben wird. Auf Grund der eigenen historischen Vergangenheit hat sich der Gesetzgeber in der Bundesrepublik Deutschland bisher klar gegen die Einführung eines aPK positioniert. Stattdessen werden mehrere bereichsspezifische Personenkennzeichen in paralleler Anwendung genutzt. Rund um deren Einführung wurde aus Sorge vor dem „gläsernen Bürger“, wie etwa bei der Steuer-ID, auch intensiv debattiert, inwieweit solche Kennzeichen genutzt werden dürfen.

Ein bereichsübergreifendes Personenkennzeichen (2wPK) im eigentlichen Sinne wird innerhalb eines Staates von Behörden nur zweier oder weniger Bereiche verwendet, um Personen eindeutig zu identifizieren. Diese Nutzung einer Kennziffer in mehreren Bereichen mag sinnvoll sein, bedarf jedoch gleichfalls einer gesetzlichen Grundlage. Zum Beispiel kann die im Bereich der Pflegeversicherung existierende Pflegeversichertennummer gemäß § 101 SGB XI ganz oder teilweise mit der Krankenversichertennummer der Krankenkassen übereinstimmen.

Bereichsspezifische Personenkennzeichen (bPK) sind zur Erfüllung öffentlicher Aufgaben in einem bestimmten Bereich der Verwaltung notwendig, um dort die relevanten Personen eindeutig identifizieren zu können. Sie werden als Kennziffern nur innerhalb dieses klar bestimmten Aufgabenbereichs des Staates von einer oder wenigen Behörden vergeben und verwendet. Jeder Bereich pflegt eine andere Systematik zur Generierung der Personenkennziffern. Für den jeweiligen Bereich können diese zentral oder dezentral (landesweit, regional oder lokal) vergeben werden. Jeder personenbezogene Datenaustausch zwischen Behörden bedarf einer gesetzlichen Grundlage und einer detaillierten Regelung. Behörden haben in der Regel keinen Zugriff auf andere bereichspezifische Personenkennziffern und die dahinterliegenden personenbezogenen Daten.

Aus diesem Grunde werden Bürger bisher bei allen Anträgen aufgefordert, auch alle erfor-derlichen Nachweise und Unterlagen mit ihren personenbezogenen Daten miteinzureichen. Diese liegen der zuständigen Stelle in der Regel nicht vor. Die Vorgehensweise entwickelte sich historisch in einer Welt von räumlich getrennten Amtsstuben. Sie entsprach den Abläufen einer papierbasierten Verwaltung, in der sich Ämter über Akten organisieren und über Vorgänge bis zur Entscheidungsfindung steuern. Die zunehmende Digitalisierung ermöglicht seit mehr als 50 Jahren einen automatisierten Datenaustausch zwischen Behörden. Dieser ist aber nur zulässig, wenn er über entsprechende Gesetze vom Gesetzgeber zur Erfüllung bestimmter öffentlicher Aufgaben etabliert worden ist. In Zeiten einer umfassenden Digitalisierung und intelligenten Vernetzung sollen künftig mit „Once-Only“ und „No-Stop-Government“, vielleicht sogar mit „No-Government“, diese aus heutiger, digitaler Sicht suboptimalen Vorgehensweisen zeitnah dauerhaft überwunden werden.[17]

Im Bereich der Gefahrenabwehr haben sich mit dem Gemeinsamen Terrorismusabwehrzentrum (GTAZ), dem Gemeinsamen Extremismus- und Terrorismusabwehrzentrum (GETZ) und dem Gemeinsamen Internetzentrum (GIZ) mehrere Kooperations- und Kommunikationsplattformen etabliert. Dort treffen sich Verbindungsbeamte verschiedener Sicherheitsbehörden regelmäßig zu Lagebesprechungen, um im Rahmen der eigenen Zuständigkeiten einen besseren Überblick über die Gesamtsituation zu gewinnen und um ihre Informationen zu Gefährdern zu verdichten. Ein allgemeines Personenkennzeichen würde diesen Plattformen die Zusammenarbeit erleichtern. Zugleich wird das Interesse an einer solchen Zusammenarbeit auch bei anderen Stellen wachsen.

Die Größe des durch ein Personenkennzeichen zu erfassenden Personenkreises variiert mit Aufgabe und Verwaltungsbereich. Erfasst werden könnten Personengruppen jeder Art, etwa alle Bundesbürger mit deutscher Staatsangehörigkeit, alle Ausländer mit einer ausländischen Staatsangehörigkeit, alle Steuerzahler, alle natürlichen Personen oder alle juristischen Personen. Am Beispiel von Personen mit zwei Staatsangehörigkeiten lässt sich zeigen, dass sich diese Personenkreise durchaus auch überschneiden könnten. Die jeweils zu erfassende Personengruppe wird im dazugehörigen Gesetz vom Gesetzgeber genau definiert.

[17] Vgl. Stocksmeier/Hunnius 2018, S. 263-264.

Große Bestände personenbezogener Daten werden heute in der Regel in Registern und den dahinterliegenden Datenbanksystemen gespeichert. Der Gesetzgeber legt in Gesetzen den Umfang der in den Registern zu speichernden personenbezogenen Daten und die Zugangsbestimmungen fest. Solche Register können sehr klein gehalten werden, so dass nur die unbedingt nötigen Daten gespeichert und verarbeitet werden. Natürlich könnten diese Register auch sehr umfangreich gestaltet werden, wenn etwa eine öffentliche Aufgabe dies erfordert. Aus einer Datenschutzperspektive wird dies aber kritisch gesehen. Der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) gebietet, darauf hinzuwirken, dass keine oder möglichst wenig personenbezogene Daten verarbeitet und gespeichert werden.[18] Das datenschutzrechtliche Gebot der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO) soll zudem sicherstellen, dass Daten nur für den Zweck verarbeitet werden, für den sie erhoben werden.

Vorstellbar ist, in einem separaten, eigenständigen Register jede Personenkennziffer um einen Basisdatensatz zu ergänzen. Ein solches Vorgehen ist besonders bei einer allgemeinen Personenkennziffer sinnvoll, da sich mit einem gemeinsam genutzten Basisdatensatz die Datenqualität in den anderen Registern verbessern lässt. Im Rahmen der Registermodernisierung soll die Datenqualität der Register von Bund, Ländern und Kommunen substanziell erhöht und dazu auf die Basisdaten des Bundeszentralamts für Steuern als Stammdaten gesetzt werden. Ziel ist es, automatisiert unzutreffende oder fehlerhafte Einträge zu identifizieren, zu korrigieren und in allen betroffenen Registern zu aktualisieren. Gegebenenfalls wird dazu auch ein persönliches Erscheinen in der kommunalen Meldebehörde erforderlich sein. Alternativ könnte man auf die Anlage von separaten Basisdatensätzen zu dem Personenkennzeichen auch verzichten und wie gehabt auf die Datenpflege in den jeweiligen Registern verweisen.

IV. Optionen für Identitätsnummernsysteme

Mit der Entscheidung für einen bestimmten Ansatz eines Personenkennzeichens fällt zugleich auch die Entscheidung über das damit verbundene Identitätsnummernsystem. Bei dessen Gestaltung gibt es grundsätzlich mehrere Optionen und Alternativen, die es in gebotener Kürze zu reflektieren gilt.

Identitätsnummernsysteme dienen dazu, größere Personengruppe derart zu erfassen, dass Personen mit einem Personenkennzeichen (im RegMoG-E: Identitätsnummer) eindeutig identifiziert werden können. Aus dem Blickwinkel der Verwaltungsinformatik und der Verwaltungswissenschaft bestehen hier einige Optionen zur Gestaltung von Identitätsnummernsystemen, die sich über einen morphologischen Kasten (**Abbildung 2**) sehr verständlich darstellen lassen.

Abb. 2 | Morphologischer Kasten zu Identitätsnummernsystemen

ID-NR-SYSTEM	AUSPRÄGUNGSFORMEN				
Typus von Personenkennzeichen	allgemeines Personenkennzeichen (aPK)	bereichsübergreifendes Personenkennzeichen (2wPK)	bereichsspezifisches Personenkennzeichen (bPK)		
Vorgehen bei der Vergabe	Personenkennzeichen zentral vergeben		Personenkennzeichen dezentral vergeben		
Inhaltliche Gestaltung des Personenkennzeichens	Steuer-ID	Andere existierende Register-ID	NEU-ID/Stammzahl in Form von einer Zufallszahl	Keine zentrale ID	
Identifizierung in anderen Registern	Steuer-ID	Bisherige Register-ID	Hashwert auf Stammzahl und Bereichs-Bezeichner	Zufallszahl	
Zu erfassende Personengruppe	Deutsche Bürger	Ausländer	Steuerzahler	Natürliche Personen	Juristische Personen
Verortung der Speicherung der Basisdatensätze zu allen Personen	Basisdatensatz beim Bundeszentralamt für Steuern (BZSt)		ohne Basisdatensatz		
Einsatz einer Intermediär-internen Datenbank mit allen bPKs	Verzicht auf Intermediär-interne ID-Datenbank		Pseudonymisierte Intermediär-interne ID-Datenbank		
Registermodernisierung	Registermodernisierungsbehörde (BVA)		Verzicht auf Registermodernisierungsbehörde		
Verortung der Intermediäre zu den BZSt-Basisdatensätzen	Intermediär zum BZSt-Basisdatensatz bei BVA (Registermodernisierungsbehörde)		Intermediär zum BZSt-Basisdatensatz bei Datenschutzaufsichtsbehörde		

[18] Vgl. Abschnitt B.IV.2

ID-NR-SYSTEM	AUSPRÄGUNGSFORMEN			
Vermittlungsstellen für Anfragen auf BZSt-Basisdatensätze	Keine Vermittlungsstelle für Anfragen	Zentrale Vermittlungsstelle für Anfragen	Verbund von Vermittlungs-stellen für Anfragen	
Prüfung der Zugriffe auf BZSt-Basisdatensätze	Keinerlei Prüfung der Zugriffe	Software-basierte Prüfung der Zugriffe	Hardware-basierte Prüfung der Zugriffe	Ständige Prüfung durch Sachbearbeiter
Freigabe von Daten durch Bürger bei bereichs-übergreifenden Abfragen	Freigabe von Daten ohne Bürgereinbindung	Anlassbezogene Freigabe von Daten durch Bürger	Freigaben von Daten stets durch Bürger erforderlich	

Grundsätzlich können Identitätsnummernsysteme auf allgemeine Personenkennzeichen (aPK), auf bereichsübergreifenden Personenkennzeichen (2wPK) oder auf bereichsspezifischen Personenkennzeichen (bPK) aufgebaut werden. Das Kennzeichen dient zur eindeutigen Identifizierung aller erfassten Personen quer über die gesamte öffentliche Verwaltung (aPK), in wenigen klar angegrenzten Bereichen der Verwaltung (2wPK) oder in einem eindeutig umgrenzten Verwaltungsbereich (bPK). Da Identitätsnummernsysteme zum Umgang mit personenbezogenen Daten verwendet werden, bedürfen sie in der Bundesrepublik Deutschland stets einer gesetzlichen Grundlage.

Die Personenkennzeichen in einem Identitätsnummernsystem können zentral oder dezentral vergeben werden. Dies hängt davon ab, ob es eine einzige Vergabestelle oder mehrere Vergabestellen, etwa bei Ländern, Bezirken, Landkreisen, Städten oder Gemeinden, geben soll. Durch technische Maßnahmen ist sicherzustellen, dass jede Identitätsnummer nur ein einziges Mal an eine Person eindeutig vergeben werden darf.

Zur inhaltlichen Gestaltung des zentralen Personenkennzeichens eignen sich verschiedene Ansätze. Diese bedienen sich entweder einer Systematik oder einfach des Zufalls. Dazu kann auf bestehenden Systematiken, wie etwa der Steuer-ID oder anderen etablierten Personenkennzeichen, aufgesetzt werden, solange dies nicht gegen geltendes Recht verstößt. Es könnten auch vollkommen neue Identitätsnummern (NEU-ID) vergeben werden, systematisch oder durch Zufallszahlen generiert. Im letzten Fall muss unbedingt sichergestellt werden, dass bei allen Zufällen keine Zahl doppelt vergeben wird. Der gewählte Ansatz sollte zur Fehlervermeidung über eine integrierte Prüfziffer verfügen. Schließlich kann auf eine zentrale Identitätsnummer zur Identifizierung auch verzichtet werden.

Zur Identifizierung von Personen in den Registern kann auf die vorhandene Steuer-ID oder die bisherige Register-ID gesetzt werden. Zudem lassen sich mit einer Hashfunktion auf Basis einer Stammzahl neuartige bereichsspezifische Personenkennzahlen generieren (vgl. dazu Abschnitt D.III). Die Alternative eine Zufallszahl besteht auch hier.

Je nach Aufgabe und Aufgabenbereich wird die zu erfassende Personengruppe unterschiedlich sein: Staatsbürger, Ausländer, Steuerzahler, natürliche Personen oder juristische Personen kommen in erster Linie in Betracht. Dies muss im Gesetz genau geregelt sein.

Zu jedem Eintrag im Identifizierungsnummernsystem können Basisdaten vorgehalten werden, etwa im Bundeszentralamt für Steuern. Dies ist denkbar, wenn mit ihrer Hilfe die Daten-qualität in den angeschlossenen Registern verbessert, eine Registerbereinigung anvisiert oder eine Registerzentralisierung verfolgt werden soll. Ein solches Basisdatenregister könnte auch nur zeitlich begrenzt für die Dauer der Datenqualitätssicherung eingerichtet werden. Aus Gründen des Datenschutzes und der Datenminimierung könnte andererseits auch auf ein Basisdatenregister verzichtet werden.

Wird auf ein aPK verzichtet, so kann mit einer pseudonymisierten und ausschließlich von einem Intermediär nutzbaren ID-Datenbank eine vergleichbare Lösung auf Basis bereichsspezifischer Personenkennzeichen realisiert werden. Sie müsste aber besonders vor Angriffen geschützt werden.

Soll eine Registermodernisierung vorgenommen werden, bedarf es einer Registermodernisierungsbehörde. Andernfalls kann auf diese verzichtet werden.

Für Zugriffe von Behörden auf Register und Basisdaten kann für die Rolle eines vertrauenswürdigen Intermediärs sowohl auf die Registermodernisierungsbehörde (beim Bundesverwaltungsamt, BVA) als auch auf die Datenschutzaufsichtsbehörde gesetzt werden.

Berechtigte Anfragen könnten ohne Vermittlungsstelle direkt an die jeweiligen Behörden, über eine zentrale Vermittlungsstelle, einen Verbund an 1+16 Vermittlungsstellen oder einen Verbund bestehender Vermittlungsstellen kommen.

Berechtigte Anfragen auf die Basisdaten beim Bundeszentralamt für Steuern müssen stets mit einem Personenkennzeichen und einem Identifier für die anfragende Stelle verbunden sein. Vor einer Rückantwort sollte die Berechtigung zur Abfrage überprüft werden. In einem geschlossenen, vertrauenswürdigen System könnte ggf. darauf verzichtet werden. In einem offenen System kann auf bewährte softwarebasierte (Passwörter, Zertifikate) und hardware-basierte Schutzmechanismen (PKI-basierte Smartcard) gesetzt werden, was aus Gründen der Beschleunigung und des Bürokratieabbaus sinnvoll erscheint. Im Hintergrund könnten zudem Überwachungssysteme laufen, die automatisch alle Anfragen der Behörden dahingehend überprüfen, ob sie zulässig sind. Allerdings darf nicht vergessen werden, dass es sich um Abfragen personenbezogener Daten handelt. Daher könnten theoretisch auch qualifizierte Sachbearbeiter die

Prüfaufgabe übernehmen. Jedoch würde dies zu einer „Engstelle“ in den Abläufen führen und den gesamten Vorgang stark verlangsamen.

Vorstellbar wäre auch eine Einbindung der Bürger in all diese Freigabeprozesse. Vielleicht würde dies viele Bürger überfordern, bei einer Vielzahl von Abfragen im Rahmen der Qualitätssicherung und Registerkonsolidierung sogar verunsichern und den Freigabeprozess auch richtig lähmen. Andererseits kann es aber Fälle geben, in denen ein Zugriff ohne den Bürger nicht gewährt werden darf, weil der Grundrechtseingriff zu groß wäre, der Bürger dann aber doch und nur ausnahmsweise einer Behörde den Zugriff etwa auf seine Krankenversicherungsdaten erlaubt. Insofern kann eine anlassbezogene Freigabe von Daten durch den Bürger in einigen Fällen eine zweite Option sein. Aus Gründen des Büro-kratieabbaus wird die Verwaltung darauf setzen, Daten ohne Freigabe durch den betroffenen Bürger zu erhalten. Aus Gründen des Datenschutzes sollte der Zugriff stets protokolliert werden und für den Bürger über das Datencockpit nachverfolgbar sein.

B. Kurzanalyse zum Entwurf des Registermodernisierungsgesetzes

I. Morphologischer Kasten der Identitätsnummer des RegMoG-Eeme

Abb. 3 | Morphologischer Kasten zum Personenkennzeichen Steuer-ID

PK / ID-NR	AUSPRÄGUNGSFORMEN				
Einzigartigkeit	einzigartig			mehrfach vergeben	
Sichtbarkeit	nicht-sprechend			sprechend	
Ziffern oder Zeichen und Umfang des Zeichensatzes	numerische Ziffernreihenfolge (0-9)			alphanumerische Zeichenreihenfolge (0-9, A-Z, a-z)	
Prüfziffer	mit Prüfziffer			ohne Prüfziffer	
Typus von Personenkennzeichen	allgemeine Verwendung (aPK: wesentliche Bereiche)		bereichsübergreifende Verwendung (2wPK: 2 oder wenige Bereiche)		bereichsspezifische Verwendung (bPK: 1 Bereich)
Vorgehen bei der Vergabe	zentrale Vergabe			dezentrale Vergabe	
Zu erfassende Personengruppe	Deutsche Bürger	Ausländer	Steuerzahler	Natürliche Personen	Juristische Personen
Basisdatensatz	mit Basisdatensatz			ohne Basisdatensatz	

Der RegMoG-E setzt auf die Steueridentifikationsnummer (Steuer-ID) nach §§ 139a, b AO als Identitätsnummer. Diese Steuer-ID (Abbildung 3) ist ein einzigartiges, nicht-sprechendes Personenkennzeichen. Sie setzt sich aus 10 Ziffern plus einer Prüfziffer zusammen. Bisher wird sie als bereichsspezifisches Personenkennzeichen der Steuerverwaltung eingesetzt. Mit dem RegMoG-E würde sie zu einem allgemeinen Personenkennzeichen (mit allen Folgen) werden.

Die Steuer-ID wird zentral vom Bundeszentralamt für Steuern an alle potentiellen Steuerzahler vergeben, was alle deutschen Staatsangehörigen, alle Unionsbürger und alle weiteren Ausländer in Deutschland umschließt. Erfasst werden so alle natürlichen Personen. Die Basisdaten werden als Stammdaten zentral beim Bundeszentralamt für Steuern gespeichert.

II. Anwendung der DSGVO und rechtlicher Prüfungsmaßstab

Die Regelungen des RegMoG-E führen zur Verarbeitung personenbezogener Daten im Sinne von Art. 4 Abs. 1 Nr. 1, 2 DSGVO, sodass der sachliche Anwendungsbereich der DSGVO nach Art. 2 Abs. 1 DSGVO grundsätzlich eröffnet ist. Informationen wie Name und Geburtsort werden der Identifikationsnummer zugeordnet, sodass diese ein personen-bezogenes Datum darstellt.[19]

Der rechtliche Entscheidungsspielraum des deutschen Bundesgesetzgebers bemisst sich daher an den Regelungen des Grundgesetzes und des Rechts der Europäischen Union. Das BVerfG sieht sich, soweit die Grundrechte des Grundgesetzes durch den Anwendungsvorrang des Unionsrechts verdrängt werden, dazu berufen, dessen Anwendung durch deutsche Stellen am Maßstab der Unionsgrundrechte neben dem deutschen Verfassungsrecht zu prüfen.[20] Prüfungsmaßstab ist daher einerseits das deutsche Verfassungsrecht, andererseits aber auch das europäische Recht. Denn das RegMoG-E nutzt die Öffnungsklausel des Art. 6 Abs. 2 und Abs. 3 DSGVO sowie des Art. 87 DSGVO (vgl. dazu auch Abschnitt B.IV). Obwohl die DSGVO als Verordnung grundsätzlich direkt anwendbar ist und kein nationales Recht vorsieht, ermöglichen ausnahmsweise die Öffnungsklauseln mitgliedstaatliche Rechtsetzung im Anwendungsbereich der DSGVO. Somit sind deutsches und europäisches Recht in diesem nicht vollständig unionsrechtlich determinierten Bereich nebeneinander anzuwenden[21]. Dies gilt auch für das Verfassungsrecht.

III. Verfassungsrecht, insbesondere Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Bereits im Mikrozensus-Urteil von 1969 stellte das BVerfG fest, dass die zwangsweise Registrierung und Katalogisierung eines Menschen durch den Staat und die hieraus folgende Objektifizierung nicht mit der Würde des Menschen vereinbar ist.[22] Hierauf aufbauend entwickelte das BVerfG 1983 im Volkszählungsurteil[23] das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. In demselben Urteil spricht das Gericht an, dass ein „einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal", das die unbeschränkte Verknüpfung von erhobenen Daten mit Datenbeständen bei Behörden ermöglicht und zur Erstellung von Persönlichkeitsprofilen führt, verfassungswidrig wäre.[24] Grundsätzlich schützt das Recht auf informationelle Selbstbestimmung vor jeder staatlichen Erhebung und Verarbeitung personenbezogener Daten,[25] ermöglicht aber zur Wahrung überwiegender verfassungsrechtlicher Werte eine Rechtfertigung von Eingriffen.

1. Einstufung und Zulässigkeit eines allgemeinen oder bereichsspezifischen Personenkennzeichens

Den soeben geschilderten Ausführungen des BVerfGs[26] zu Personenkennzeichen wird ein generelles Verbot von Personenkennzeichen nicht entnommen.[27] Vor diesem Hintergrund unterscheidet die Literatur zwischen *allgemeinen* und *bereichsspezifischen* Personenkennzeichen.[28] Danach sind allgemeine Personenkennzeichen als grundsätzlich verfassungswidrig einzustufen. Denn sie würden die vom BVerfG ausdrücklich erwähnte, abzulehnende Zusammenführung der bei den Verwaltungsbehörden vorhandenen Datenbeständen ermöglichen. So sieht etwa der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) die Einführung eines zentralen Personenkennzeichens an sich als verfassungswidrig an[29], hält dagegen den Einsatz von bereichsspezifischen Kennzeichen mit entsprechenden technischen Sicherheitsvorkehrungen aber für grundsätzlich möglich.[30]

Die Identifikationsnummer in ihrer gegenwärtigen Form ist ein bereichsspezifisches Personenkennzeichen.[31] Auch der Bundesfinanzhof urteilte 2012, dass die Identifikationsnummer nach § 139a AO zumindest zu jenem Zeitpunkt verfassungsrechtlichen Ansprüchen genüge.[32] Hierbei unterstreicht die Urteilsbegründung, dass die Identifikationsnummer nur zu steuerlichen Zwecken verwendet werden darf, sodass die genannten Bedenken gegenüber einem allgemeinen Personenkennzeichnen hier nicht zum Tragen kamen.[33] Der Hinweis in der Begründung des Gesetzentwurfs auf die höchstrichterlich bestätigte Verfassungskonformität der Steueridentifikationsnummer als Grundlage für die Reform[34] ist insofern nicht zutreffend.[35]

Nach dem IDNrG-E soll die Identifikationsnummer nunmehr bei über 50 Registern als zusätzliches Ordnungsmerkmal eingetragen werden. Zwar konnten 2017 bundesweit 214 verschiedene Register verzeichnet werden[36]; die vom Entwurf betroffenen Register entstammen jedoch unterschiedlichsten Lebensbereichen, z.B. den Versicherungskonten der Rentenversicherungsträger, der Grundsicherung für Arbeitssuchende, der gesetzlichen Unfallversicherung, der Fahreignung, der Handwerksrolle, den allgemeinbildenden und beruflichen Schulen/Ausbildungswesen, dem Waffenregister, der Gewährung von Elterngeld, Insolvenzen, Aufenthaltsberechtigungen oder auch dem Liegenschaftskataster. Selbst § 7 Abs. 2 IDNrG-E geht von einer Einteilung in zumindest sechs unterschiedliche Verwaltungsbereiche aus.[37]

[19] *Martini/Wagner/Wenzel* 2017, S. 5 m.w.N; Wiss. Dienst BTag 2020, Gutachten, S. 5 f.
[20] BVerfG NJW 2020, 314 (1. Leitsatz).
[21] Vgl. BVerfG NJW 2020, 300 Rn. 41 f.
[22] BVerfGE 27, 1, 6.
[23] BVerfGE 65, 1 ff.
[24] BVerfGE 65, 1, 53.
[25] *Di Fabio*, in: Maunz/Dürig 2020, Art. 2 f., Rn. 176.
[26] BVerfGE 65, 1, 53.
[27] *Martini/Wagner/Wenzel* 2017, S. 30.
[28] *Martini/Wagner/Wenzel* 2017, S. 30 f. m.w.N.; der gleichen Einteilung folgt *Wiss. Dienst* BTag, Gutachten, S. 14 ff.
[29] *BfDI* 2020, S. 4.
[30] Vgl. *BfDI* 2020, S. 8
[31] Vgl. *Martini/Wagner/Wenzel* 2017, S. 30 f.
[32] *BFH* 2012, Urt. v. 18.1.2012 – II R 49/10.
[33] *Humanistische Union* 2020, S. 8 mit Verweis auf BFH, Urteil vom 18.1.2012 – II R 49/10 Rn. 59 ff.
[34] RegMoG-E, S. 72.
[35] *BfDI* 2020, S. 7, Humanistische Union 2008, S. 8.
[36] *Statistisches Bundesamt* 2017, S. 4.
[37] Beispielhaft genannt werden Inneres, Justiz, Wirtschaft und Finanzen, Arbeit und Soziales, Gesundheit, Statistik, RegMoG-E, S. 81.

Jedenfalls kann ein allgemeines Kennzeichen nicht nur dann vorliegen, wenn alle oder ein Großteil der nationalen Register das Kennzeichen als zusätzliches Ordnungsmerkmal aufnehmen müssen. Ein rein quantitativer Maßstab führt zu großem Missbrauchspotential, da bestimmte Register gezielt ausgelassen werden könnten, um den höheren verfassungsrechtlichen Maßstab zu umgehen. Umgekehrt ist ein allgemeines Personenkennzeichen nicht bereits dann gegeben, wenn mehr als ein Bereich erfasst ist. Sobald allerdings – wie vorliegend – eine Vielzahl von wesentlichen Lebensbereichen über eine gemeinsame Personenkennziffer verknüpft wird, ist von einem allgemeinen Kennzeichen auszugehen.[38] Demnach wäre deren Erweiterung, wie im RegModG-E vorgesehen, grundsätzlich als sehr problematisch anzusehen.

Als alternative Lesart wird teilweise vertreten, dass das BVerfG – insbesondere vor dem Hintergrund der Strahlkraft des Urteils – nur die Profilbildung als solche ausschließen wollte.[39] Verfassungswidrig seien vielmehr die Verknüpfungsmöglichkeiten personenbezogener Daten, die sich aus der Einführung eines Personenkennzeichens ergeben.[40] Ferner seien heutzutage durch den technischen Fortschritt viele weitere Möglichkeiten zur Profilbildung ohne weiteres verfügbar, sodass sich die Frage stellt, ob ein Verbot eines Personenkennzeichens überhaupt diesen Zweck erreichen kann. Sinnvoller sei hingegen die Erörterung technischer und organisatorischer Mittel, welche die Gefahren aus der Profilbildung reduzieren können.[41] Aber auch nach dieser Auffassung sind die Grenzen, die das BVerfG aufgezeigt hat, überschritten. Denn die Breite der verknüpften Register und damit die Abrufmöglichkeiten der darüber erschließungsfähigen Daten dringen in den Bereich der Profilbildung vor. Diese wird von der DSGVO an verschiedenen Stellen als eine besonders problematische Datenverarbeitung mit hohen Risiken eingestuft.[42]

Die weiter unten (Teil D) vorgeschlagenen Alternativen schränken zwar die Abrufmöglichkeiten per se nicht ein; dies wäre der wirkungsvollste Schutz. Sie erschweren aber die Umgehung des vorgesehenen Prozesses und damit eine zu Lasten des Bürgers wirkende Verknüpfung der Daten ohne Zweckbindung und Kontrollmöglichkeit. Damit wird auch der Missbrauch durch Dritte und auch ein Identitätsdiebstahl erschwert, wie er beispielsweise in Staaten mit allgemeinen Personenkennzeichen wie den USA mit der Social Security Number vorkommt und dort eine große Gefahr darstellt.

2. Verfassungswidrigkeit der Ermächtigung zum Erlass einer Rechtsverordnung in § 7 Abs. 2 S. 2 IDNrG-E

Für Datenübermittlungen zwischen öffentlichen Stellen verschiedener Bereiche sieht § 7 Abs. 2 S. 2 IDNrG-E i.V.m. § 12 Abs. 1 Nr. 2 eine Rechtsverordnungsermächtigung zugunsten der Bundesregierung vor. Rechtsverordnungen unterliegen gemäß Art. 80 Abs. 1 S. 2 GG erheblichen Anforderungen, um der damit verbundenen Delegation von gesetzgeberischen Aufgaben an die Exekutive und damit einer verfassungsrechtlich unerwünschten Durchbrechung des Gewaltenteilungsprinzips nach Art. 20 Abs. 3 GG entgegenzuwirken; das Wesentlichkeitsprinzip dient also der negativen Kompetenzabgrenzung.[43] Die Beantwortung der (politischen) Kernfrage, ob die Verwaltung handeln darf, liegt beim Gesetzgeber. Grundsätzlich gilt, dass der Gesetzgeber *„alle Fragen, die für die Ausübung der Grundrechte wesentlich sind, unabhängig davon, ob im konkreten Fall Freiheitsrechte oder Gleichheitsrechte betroffen sind“*, selbst zu regeln hat.[44]

Die Einführung einer Personenkennziffer für alle Bürger und Steuerzahler, wie vom RegMoG-E vorgesehen, berührt in erheblicher Weise das Recht auf informationelle Selbst-bestimmung und ist vom BVerfG kritisch beurteilt worden[45].

Die Einordnung von Datenbeständen in Bereiche i.S.d. RegMoG-E hat erhebliche Auswirkungen auf das Verfahren der Datenübermittlung und die Möglichkeit des Rechtsschutzes für betroffene Bürger, zumal nach § 7 Abs. 2 S. 7 IDNrG-E die Datenübermittlung innerhalb von Bereichen privilegiert verlaufen soll. Erfolgt also eine – grundsätzlich zulässige – Delegation der näheren Ausgestaltung nach Art. 80 Abs. 1 S. 2 GG, muss der Gesetzgeber in besonderem Maße Inhalt, Zweck und Ausmaß vorgeben. Dies ist aber nicht der Fall. Weder hat der Gesetzgeber vorgeben, welche Kriterien zur Bestimmung von Bereichen herangezogen werden sollen, noch hat er die Zahl bestimmt (lediglich die Untergrenze von sechs Bereichen ist benannt), noch hat er vorgegeben, welche Zielsetzung mit der Bereichs-aufteilung einhergehen soll. Die Rechtsverordnungsermächtigung nach § 12 Abs. 1 Nr. 2 IDNrG-E erwähnt allerdings allein Anzahl und Abgrenzung.

Ebenfalls verstößt die Verordnungsermächtigung in § 12 Abs. 3 IDNrG-E gegen Art. 80 Abs. 1 S. 2 GG. Danach kann „das jeweils zuständige Bundesministerium“ das Verfahren nach § 7 Abs. 2 IDNrG-E auch für Datenübermittlungen innerhalb eines Verwaltungsbereichs bestimmen. Dem lässt sich entnehmen, dass der Gesetzgeber davon ausgeht, dass Verwaltungsbereiche sich einem Bundesministerium zuordnen lassen. Allerdings – wie etwa der Zuschnitt des Bundes-

[38] Im Ergebnis ebenso BfDI, 2020, S. 8; wohl auch Humanistische Union 2020, S. 7 f.; Wiss. Dienst BTag, 2020, Gutachten, S. 16 f. nimmt zwar ein allgemeines Personenkennzeichen an, trifft jedoch keine verbindliche Aussage zu dessen Zulässigkeit.
[39] *Martini/Wagner/Wenzel* 2017, S. 31 ff.
[40] *Martini/Wagner/Wenzel* 2017, S. 31
[41] *Hornung* 2005, S. 161 f.; ebenso Martini/Wagner/Wenzel 2017, S. 33.
[42] *Scholz*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art.4 Nr. 4, Rn. 1.
[43] Vgl. *Voßkuhle*, JuS 2001, 118 f.
[44] Vgl. BVerfGE 47, Rn. 99.
[45] Siehe oben Einstufung und Zulässigkeit eines allgemeinen oder bereichsspezifischen Personenkennzeichens.

ministeriums des Innern, für Bau und Heimat illustriert – ändern sich zum einen Zuständigkeiten von Bundesministerien, zum anderen sind sie oft so breit aufgestellt, dass man nicht von lediglich einem Bereich ausgehen kann. Das Baurecht und das Sicherheitsrecht sind nach grundständigem Verständnis unterschiedliche Verwaltungsmaterien; nach welchen Kriterien hier ein Verwaltungsbereich angenommen werden soll, bleibt offen und verstößt damit – auch unter Bestimmtheitsanforderungen nach Art. 20 Abs. 3 GG – gegen das Grundgesetz.

3. Verhältnismäßigkeit eines Eingriffs in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Folgt man der Ansicht nicht, dass die Einführung eines allgemeinen Personenkennzeichens bereits grundsätzlich als verfassungswidrig einzustufen ist, wäre der Eingriff in das allgemeine Persönlichkeitsrecht in der Ausprägung des Rechts auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1, Art. 1 Abs. 1 GG jedenfalls unverhältnismäßig.

a) Legitimes Ziel und seine Bedeutung

Das RegMoG-E soll die Funktions- und Leistungsfähigkeit sowie die Effektivität der Verwaltung verbessern und in Vorbereitung des sogenannten Once-Only-Prinzips auch zu einer Entlastung und Vereinfachung der Bürger in der Kommunikation mit der Verwaltung führen.[47] Ferner soll ein registerbasierter Zensus ermöglicht werden.[48]

Wie eingangs geschildert, gehen die Ziele allerdings noch deutlich darüber hinaus. Mittel- und langfristig ist mit dem RegMoG-E der erste Schritt zu gänzlich neuartigen Governance-Modellen eröffnet, die allerdings ganz erheblichen verfassungsrechtlichen Bedenken begegnen, auch wenn sie sich im Gewand der Kosteneinsparung, des bürgernahen schlanken Staats und der Effizienzgewinne präsentieren.[49] Deutlich wird dies unmittelbar über § 16 IDNrG-E, in dem weitere Ziele bekannt gemacht werden: Damit wird ersichtlich auch eine Verbreiterung des Datenaustauschs nicht nur innerhalb der Verwaltung und mit dem Bürger angestrebt, sondern eine breite Verwendung der Identifikationsnummer – letztlich auch für den privaten Bereich.

Hierbei handelt es sich im geschilderten ersten Schritt von Kosteneinsparung, Vereinfachung von Verwaltungsvorgängen und Zensusermöglichung um legitime Ziele der Effektivität der Verwaltung, der Akzeptanzsteigerung der Kommunikation zwischen Bürger und Staat und der Vereinfachung und Anpassung von Verwaltungsvorgängen. Diese Ziele können allerdings kein sonderlich großes Gewicht beanspruchen; sie sind verfassungsrechtlich nicht geboten und werden von Schutzpflichten, die von Grundrechten ausgehen, nicht erfasst. Europarechtlich mag in einzelnen Fällen die Nutzung von bereichsspezifischen Personenkennziffern vorgegeben sein; eine allgemeine, dem Anwendungsvorrang unterfallende Verpflichtung zur Einführung einheitlicher Personenkennzeichen lässt sich aber daraus nicht ableiten.

Es ist durchaus sehr zweifelhaft, ob die dahinterstehenden weitreichenden Ziele des Once-Only- und des No-Stop-Governments mit einem demokratischen freiheitlichen Rechtsstaat überhaupt in Einklang gebracht werden können angesichts der damit einhergehenden Machtverschiebungen, Verletzung der Kernelemente von Persönlichkeits- und Datenschutzrechten sowie Standardisierung mit Aufgabe von Minderheitenschutz.[50]

b) Geeignetheit und Erforderlichkeit

Eine Personenkennziffer, wie vom RegMoG-E vorgesehen, steigert auch die Wahrscheinlichkeit der Verwirklichung dieser eben skizzierten begrenzten Ziele des ersten Schritts und ist daher geeignet.

Hinsichtlich eines gleich effektiven, milderen Mittels stellen sich allerdings erhebliche Zweifel, gibt es doch weitere Alternativen, die weniger eingriffsintensiv eine Verwaltungsmodernisierung im Registerwesen voranbringen.

Das RegModG-E verfolgt ein Konzept des 4-Corner-Modells mit „doppeltem Umschlag". Die weiterleitende Stelle nach § 7 IDNrG-E kann also die Inhalte nicht zur Kenntnis, sondern lediglich die Metadaten, die zur Erfüllung der Vermittlung erforderlich sind. Dadurch, dass solche Zwischenstellen vorgesehen sind, ist für die registerführenden Behörden eine gemeinsame Identifikationsnummer – wie sie das RegModG-E einführen soll – nicht erforderlich. Dies gilt umso mehr, als technische Ausgestaltungsmöglichkeiten weitere Beschränkungen erlauben, ohne die Funktionalität einzuschränken.[51]

So lässt sich auf das österreichische Modell des zentralen Identitätsmanagements bei Behörden verweisen, ohne hier in Details zu gehen:[52] In Österreich wird jeder natürlichen Person eine sog. „Stammzahl" zugeordnet, die allerdings nur einer einzigen zentralen Instanz, der Stammzahlenregisterbehörde[53], vorliegt. Diese Stammzahl wird jedoch mit keinen weiteren personenbezogenen Daten verknüpft. Anhand dieser Stammzahl werden mittels eines Algorithmus bereichsspezifische Kennzahlen erstellt, die von den jeweiligen Fachregistern aufbewahrt werden. Möchte eine Behörde Daten von einer anderen Behörde abrufen, schickt sie ihre bereichsspezifische Kennzahl in verschlüsselter Form an die Stammzahlenregisterbehörde. Diese wiederum stellt die bereichsspezifische Kennzahl der anderen Behörde in verschlüsselter Form zur Verfügung. Mit beiden Kennzahlen kann die abfragende Behörde nun die Daten bei der anderen Behörde beantragen.

[46] Dazu gleich noch unten unter B.3.c)(5).
[47] Vgl. RegMoG-E, S. 37 und S. 70.
[48] RegMoG-E, S. 70 f.
[49] Siehe dazu auch noch unten unter B.3.c)(5).
[50] Siehe dazu noch unten unter B.3.c)(5).
[51] Siehe dazu unten Teil D.
[52] Siehe dazu unten Teil D.
[53] Bis 28.12.2018 war dies die Datenschutzbehörde der Bundesrepublik Österreich. Nun ist das Bundesministerium für Digitalisierung und Wirtschaftsstandort die neue Stammzahlenregister-behörde, vgl. https://www.dsb.gv.at/aufgaben-taetigkeiten/stammzahlenregisterbehoerde.html.

Bei der Übertragung der Daten schickt die andere Behörde die verschlüsselte Kennzahl der ersten Behörde mit, damit diese die Daten zuordnen kann. Zu keinem Zeitpunkt erlangt eine der beiden Behörden Kenntnis über die (unverschlüsselte) bereichsspezifische Kennzahl der anderen Behörde.[54] Ein solches Vorgehen kann die zuvor benannten Risiken der staatlich veranlassten Profilbildung und eines ungehinderten Zugriffs auf Bürgerdaten deutlich reduzieren; es ist gleich geeignet und somit ein milderes Mittel.

Das RegMoG-E geht in der Begründung zwar auf das österreichische Modell ein, lehnt dieses jedoch aufgrund „größerer rechtlicher, technischer und organisatorischer Komplexität" und den außerordentlichen Kosten- und Zeitaufwand ohne weitere Nachweise ab.[55] Die Überzeugungskraft dieses Arguments ist fraglich: Es besteht (mit dem österreichischen Modell) bereits im deutschsprachigen Raum ein funktionierendes, weniger eingriffsintensives Instrument, das angesichts digitalisierter Abläufe schnell und effektiv eingesetzt werden kann. Die Datenschutzkonferenz (DSK) hat daher zu Recht dazu aufgefordert, ein solches Modell für Deutschland ernsthaft zu prüfen.[56]

Zudem zeigt das vorliegende Gutachten im Folgenden eine Reihe von Alternativen auf und entwickelt einzelne davon in Tiefe und Breite.[57] Diesen lässt sich entnehmen, dass die vom Gesetz vorgesehene Einführung einer Identifikationsnummer nicht alternativlos ist, sondern vielmehr die Ziele des Gesetzgebers auch auf anderen, weniger eingriffsintensiven Wegen erreicht werden können.

c) Angemessenheit

Sollten die vorgestellten Alternativen trotzdem als weniger effektiv erachtet und damit die Erforderlichkeit des im Gesetzesentwurf vorgesehenen deutschen Wegs des RegMoG-E bejaht werden, wäre auch die Angemessenheit kritisch zu betrachten.[58] Tatsächlich sprechen gute Gründe dafür, davon auszugehen, dass eine zentrale Identifikationsnummer den verfassungsrechtlichen Test der Angemessenheit nicht besteht.

Im Rahmen der Angemessenheit erfolgt eine Abwägung zwischen der Schwere des Eingriffs in die Grundrechte, allen voran in das Recht auf informationelle Selbstbestimmung, und der Intensität des verfolgten Ziels. Dabei kann der Gesetzgeber Ausgleichsmaßnahmen vorsehen, mittels derer die eigentliche Schwere des Eingriffs abgemildert und somit die Interessenabwägung zugunsten der Verwirklichung des Ziels verschoben wird.

(1) Eingriffsintensität in das Recht auf informationelle Selbstbestimmung

In seiner Rechtsprechung hat das BVerfG verschiedene Parameter festgelegt, die zur Bestimmung der Eingriffsintensität in das Recht auf informationelle Selbstbestimmung herangezogen werden können. Allen voran bemisst sich die Schwere eines Eingriffs an Art bzw. Qualität, Umfang bzw. Quantität, Verwendung bzw. Kontext und Missbrauchspotenzial bzw. negativen Konsequenzen der Daten und ihrer Verarbeitung.[59]

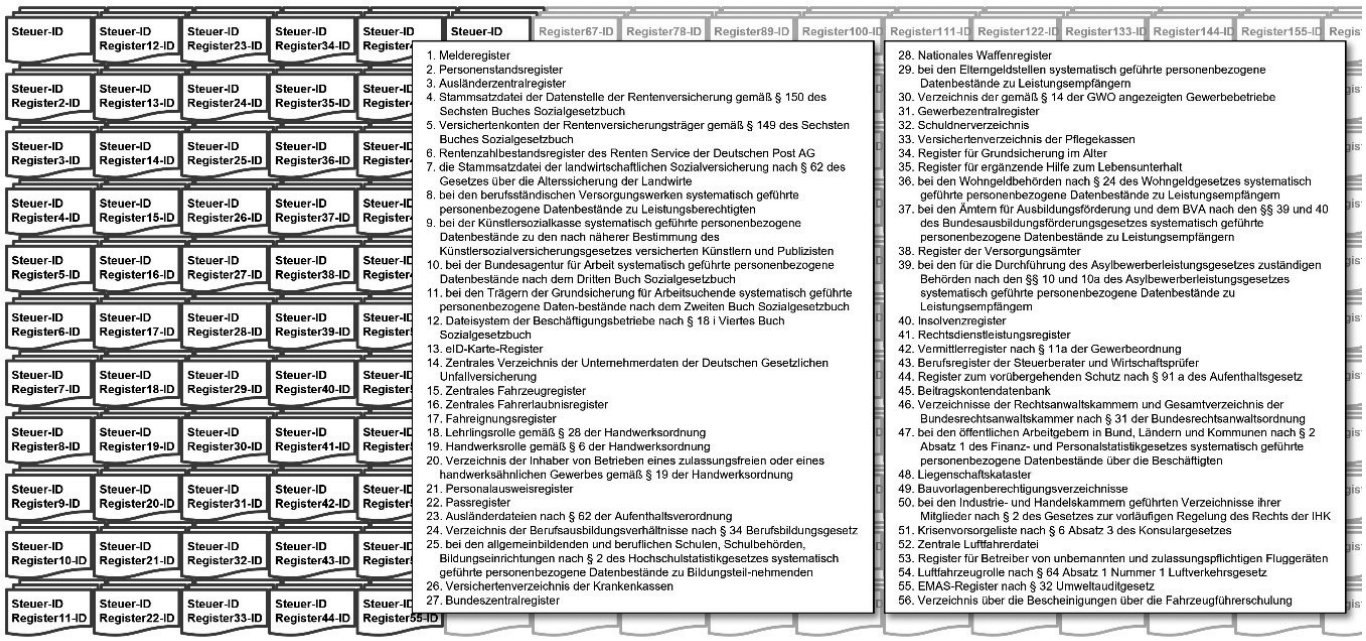
Der Umfang des Eingriffs durch die Anwendung auf die schon jetzt über 50 im Anhang des IDNrG-E gelisteten Register aus verschiedensten Lebensbereichen ist beträchtlich. Die Verwendungsbereiche könnten mit einfachem Gesetz auch erweitert werden. Neuartige Register ließen sich mühelos aufbauen und integrieren. So könnte zukünftig auch der Datenbestand und die Pseudonyme des Forschungsdatenzentrum erschlossen werden, das über § 303d Digitales Versorgungsgesetz (DVG) für wesentliche Daten aller gesetzlich Versicherten eingerichtet werden soll.[60] Die Quantität der damit verarbeitbaren und zugänglichen Daten ist uferlos groß.

Auch der betroffene Personenkreis ist als außerordentlich groß einzustufen: Gemäß § 139a Abs. 1 S. 1 AO in Art. 3 RegMoG-E betrifft dies künftig alle Steuerpflichtigen und jede sonstige natürliche Person, die bei einer öffentlichen Stelle ein Verwaltungsverfahren führt. Durch diese Regelung ist von einer Zuteilung der Identifikationsnummer an nahezu alle natürlichen Personen auf Bundesgebiet auszugehen. Ein quantitativ größerer Eingriff ist kaum vorstellbar; er entspricht dem Personenkreis, den das BVerfG in den Volkszählungs- und Mikrozensusurteilen betrachtet und als zu weitreichend beurteilt hat.

Alleine die Möglichkeiten, die dadurch entstehen, innerhalb von Minuten mit einem handelsüblichen Laptop die Daten von mehr als 83 Millionen Bürgern und Steuerpflichtigen schon jetzt aus 57 Registern verknüpfen und dann mit gezielten Anfragen auswerten zu können, sind nicht mehr überschaubar, geschweige denn vorhersehbar, und können kaum gerechtfertigt werden.

[54] Vgl. zu diesem Absatz Ausführungen und Schaubild von Nationaler Normenkontrollrat 2017, S. 42 f.; für weitere Details, insbesondere in rechtlicher Hinsicht s. *Martini/Wagner/Wenzel* 2017, S. 36 ff.
[55] Vgl. RegMoG-E, S. 38
[56] *DSK* 2020, S. 2.
[57] Siehe unten Teil D.
[58] Vgl auch *Wiss. Dienst BTag* 2020, Gutachten, S. 22: „offen".
[59] Vgl. BVerfG NJW 2020, 2699, 2707.
[60] Siehe oben Abschnitt A.II

Abb. 4 | Gesamtüberblick der künftig über die Steuer-ID erschließbaren Register



Zusätzliche Sorge bereitet der Drang vieler Software- und Plattformanbieter, ihre Software cloud-basiert als Service über eine Plattform anzubieten und gleichzeitig ihre Kunden zu einer Öffnung ihrer Datenbestände zu drängen. Sollte eine Behörde in Zukunft, etwa für eine komplexe KI-basierte Analyse von personenbezogenen Datenbeständen, die weltweit nur ein einziger Anbieter beherrscht, Dritten einen Zugang zu ihren bisher geschützten Registern eröffnen müssen, lassen sich auch diese Folgen nicht mehr überschauen. Ein solcher Dienst könnte selbst zu wesentlichen neuen Erkenntnissen auf Grundlage der allgemeinen Personenkennzeichen gelangen und künftig immer wieder gezielt nach dem Personenkennzeichen suchen. Vielleicht sähe ein solcher Algorithmus es sogar als erforderlich an, sich Kopien aller relevanten Datensätze mit den Personenkennzeichen anzufertigen, um noch bessere Ergebnisse zu erzielen. Zumindest hätten ausländische Nachrichtendienste, in deren Staaten solche Anbieter ansässig sind, ebenfalls ein großes Interesse an diesen Beständen. Gerade für den Bereich der Inneren Sicherheit lässt sich nicht dauerhaft ausschließen, dass einige verantwortliche Stellen entsprechende Analysedienste nutzen werden.[61]

Die Intensität eines Eingriffs nimmt insbesondere mit der Möglichkeit von Folgeeingriffen und anderen Maßnahmen, die aus der Verknüpfung von Datensätzen resultieren, zu.[62] Zwar sind die zu übermittelnden Daten in § 4 Abs. 2 und 3 IDNrG-E grundsätzlich begrenzt; die potentielle Verbindung mit den Daten aus den verschiedenen Registern führt jedoch zu einem höheren Risiko. Insbesondere das Datum des letzten Verwaltungskontakts gemäß § 4 Abs. 3 Nr. 2 kann zur Gefahr eines übergreifenden Trackings und einer Profilbildung durch die Behörden führen.[63] Daher ist, sollte man der oben genannten Ansicht folgen, dass das BVerfG im Volkszählungsurteil nicht generell gegen allgemeine Personenkennzeichen entschieden hat, sondern lediglich einer Profilbildung entgegenwirken wollte, jedenfalls darüber die Schwelle der Zulässigkeit nach dieser Rechtsprechung überschritten.

Dies gilt erst recht, weil die Registermodernisierungsbehörde im Rahmen ihrer Aufgaben auch Qualitätssicherung der Datenbestände vorsehen soll. Dazu erfolgt gem. § 7 Abs. 1 S. 2 IDNrG-E eine Prüfung auf Vollständigkeit und Schlüssigkeit, ohne dass hierfür eine vergleichbare Regelung wie bei Datenübermittlungen unter Nutzung der Identifikationsnummer nach § 7 Abs. 2 IDNrG-E durch Vermittlungsstellen vorgesehen ist – nämlich dass dies ohne Kenntnis der Nachrichteninhalte erfolgen soll, also nach dem 4-Corner-Modell mit doppeltem Umschlag. Selbst wenn man davon ausgehen sollte, dass dies auch für Abs. 1 vorgesehen ist, ist die Bedeutung dieser Schutzmaßnahme so gewichtig, dass der Gesetzgeber sie hätte vorsehen müssen, um deren Anwendung auch in der Registermodernisierungsbehörde sicherzustellen.[64] Denn mit der Möglichkeit der Kenntnisnahme von allen Abfragen entsteht auf Meta- und Inhaltsebene eine erhebliche Gefahr für eine Profilbildung über Bürger.

Weitere Kriterien der Rechtsprechung zur Beurteilung der Eingriffsintensität sind die Veranlassung eines Eingriffs bzw. ein Vorkontakt.[65] Im Gegensatz zur Auffassung des *Wissenschaft-*

[61] Vgl. oben Abschnitt A.II
[62] BVerfG NJW 2008, 1505, 1508.
[63] Vgl. GI 2020, S. 6.
[64] Auf die Sicherheitsmaßnahmen gehen wir in Teil D erneut ein.
[65] Vgl. BVerfG NJW 2020, 2699, 2707.

lichen Dienstes des Bundestages[66] kann es aber vorliegend keinen Unterschied hinsichtlich Eingriffsintensität zwischen einem durch eine Bürgerin angestoßenen Verwaltungsverfahren und der Prüfung der Register ohne Anlass durch diesen selbst geben. In vielen Lebensbereichen (bspw. beim Führen eines KFZ oder dem Erwerb einer Immobilie) ist wegen des gesetzlichen Erlaubnisvorbehalts ein Verwaltungskontakt notwendig, um individuelle Freiheiten auszuüben. In solchen Fällen gibt es keine Möglichkeit, den Eingriff zu verhindern; insbesondere ist keine Opt-out-Möglichkeit vorgesehen. Insofern ist die Annahme eines weniger intensiven Eingriffs hier verfehlt. Zudem fehlt es gerade an der zurechenbaren Veranlassung: Die Steuer-ID wird bereits für Kinder mit der Geburt vergeben, ohne dass eine Steuerpflicht vorliegt.

Hinsichtlich der intensitätserhöhenden Heimlichkeit[67] des Eingriffs ist zwar positiv hervorzuheben, dass mit dem Datencockpit nach § 10 OZG-E eine Möglichkeit des Bürgers geschaffen wird, sämtliche Eingriffe nachzuvollziehen. Dennoch ist der eigentliche Eingriff zunächst ohne Kenntnis des Betroffenen möglich und vorgesehen. Sollte es zu einer missbräuchlichen Verwendung der Identifikationsnummer kommen, ist eine Feststellung und das Ersuchen von Rechtsschutz nur im Nachgang möglich. Dies ist bei Informationen zusätzlich problematisch, da hier ein zwangsweises Vergessen kaum möglich ist und daher Eingriffe grundsätzlich irreversibel sind. Bei einer rein nachträglichen Kontrolle ist auch zu beachten, dass die Hemmschwelle zur Nachprüfung seitens betroffener Bürger steigen könnte.

Der RegMoG-E berücksichtigt zudem nicht, dass für einzelne Personen besondere Anforderungen an den Schutz aus persönlichkeitsrechtlichen, betriebsspezifische oder auch, lebens- und gesundheitsrechtlichen Gründen bestehen können. In diversen Registern besteht daher die Möglichkeit von Sperrvermerken, für deren Übernahme in die neu geschaffenen Verfahren keine Vorkehrungen getroffen sind.[68]

Schließlich werden schon über die Basisdaten auch besondere Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO (Sterbetag, § 4 Abs. 2 Nr. 10 IDNrG-E) oder Art. 3 I GG (Geschlecht, § 4 Abs. 2 Nr. 7 IDNrG-E) zugeordnet und gespeichert, denen ein besonderes Diskriminierungspotential innewohnt. Über die Verknüpfung mit den diversen Registern erfolgen zudem Zugriffe auf weitere besondere Daten, mindestens über die Register nach Nr. 2., 4.-12. sowie 29. und 33.-35. Schließlich sind eine Reihe der in den Registern vorgehaltenen und über die Identifikationsnummer erreichbaren Daten in besonderer Weise als persönlichkeitsrelevant einzustufen, weil sie essentielle, üblicherweise von besonderen Geheimhaltungsverpflichtungen wie dem Sozialgeheimnis erfasste Informationen über das Leben der Bürger offenbaren können.

(2) Zweckbindung

Verpflichtet der Gesetzgeber Behörden dazu, Datenbestände anzulegen, muss er das verfassungsrechtlich bedingte Gebot der Zweckbindung beachten.[69] Der Gesetzgeber ist zudem verpflichtet, durch ergänzende Folgeregelungen festzustellen, dass eine Erweiterung der Verwendungsmöglichkeiten unter Umgehung des Zweckbindungsgebots nicht stattfindet.[70] Wie der Entwurf eine solche schleichende Erweiterung der Anwendungsbereiche der Identifikationsnummer verhindern will, ist unklar. Ohne weiteres können weitere Register verknüpft werden. Als schlechtes Vorbild dient ausgerechnet die Steueridentifikationsnummer selbst, bei deren Einführung ausdrücklich versichert wurde, dass eine Ausweitung auf andere Lebensbereiche nicht stattfinden würde.[71] Angesichts einer strengen Zweckbindung ist auch nicht ausreichend, dass das IDNrG-E als solches in § 5 Abs. 1 Nr. 1 und 2 lediglich Zuteilung und Abruf der Daten vorsieht. Genauso ist der Verweis in § 6 Abs. 2 IDNrG-E auf andere Rechtsgrundlagen für Verarbeitungen anhand der Identifikationsnummern dem Maßstab des BVerfG nicht angemessen. Die mangelnde Zweckbindung führt dazu, dass auch Private die Identifikationsnummer verwenden können.[72] Daher sollte der Entwurf die privatwirtschaftliche Nutzung der Identifikationsnummer ausdrücklich verbieten, um einer Profilbildung durch Unternehmen vorzubeugen.[73]

Verstärkend kommen noch die besonderen Bindungen der Steuerverwaltung hinzu. Sie darf für ihre Besteuerungsverfahren keine allgemeinen Personenkennzeichen verwenden. Ein angenommener Gesetzesentwurf würde damit auch die Grundlagen der Steuererhebung zerstören und unerwünschte Folgewirkungen für die Finanzierung des Staates auslösen.[74]

Dass ein gesetzliches Verbot der Verknüpfung eines Kennzeichens mit anderen Datenbeständen oder Kennziffern durchaus auch ausdrücklich gesetzlich festgeschrieben werden kann, zeigt die Regelung zur Krankenversichertennummer.[75] Bereits bei deren Einführung bestand die Befürchtung, dass eine Verknüpfung mit der Rentenversicherungsnummer zum Entstehen eines unzulässigen Personenkennzeichens führen könnte.[76] Aus diesem Grund erließ der Gesetzgeber die Regelung in § 290 Abs. 1 S. 4 SGB V, die eine Verbindung der beiden Nummern explizit verbietet.

(3) Unbestimmter Missbrauchsschutz

Einer missbräuchlichen Verwendung der Daten trägt das IDNrG-E durch Strafvorschriften in § 17 IDNrG-E und technischen Schutzvorkehrungen in § 7 Abs. 2 IDNrG-E in gewissem Umfang Rechnung.[77] Allerdings spezifiziert § 8 Abs. 2 S. 1 IDNrG-E nicht, welche technischen und organisatorischen Maßnahmen die Registermodernisierungsbehörde zu ergreifen hat, und auch die abrufende Stelle wird nach

[66] Wiss. Dienst BTag, Gutachten, S. 21.
[67] BVerfG NJW 2020, 2699, 2707.
[68] BRat 2020, S. 10 ff.
[69] BVerfG NJW 2020, 2699, 2708.
[70] BVerfG NJW 2020, 2699, 2708.
[71] Vgl. *Schaar*, ZD 2011, 49.
[72] *Wiss. Dienst BTag* 2020, Gutachten S. 21.
[73] Vgl. auch *DAV* 2020, S. 5.
[74] Siehe auch *BRat* 2020, S. 2
[75] Vgl. *Hornung* 2005, S. 162.
[76] *BfDI* 2004, S. 165.
[77] *Wiss. Dienst BTag* 2020, Gutachten, S. 21.

§ 8 Abs. 2 S. 2 IDNrG-E nur unbestimmt verpflichtet sicherzustellen, dass nur befugte Personen die Daten abrufen können. Angesichts der hohen Eingriffsintensität steigen aber auch die Anforderungen an die Bestimmtheit der gesetzgeberischen Regelungen. Eine generelle Aussage, welche die Verantwortung vollständig auf die Behörden auslagert und nur die Verpflichtung aus der DSGVO wiederholt, genügt diesen Anforderungen nicht. Zudem fehlt es an einer konkretisierten Verpflichtung zur beständigen Anpassung und Überprüfung.[78] Die Überprüfung durch den BfDI nach § 13 IDNrG-E kann interne Vorgänge nicht ersetzen.

Zudem wird zwar keine sprechende Personenkennziffer vorgesehen, wohl aber eine offene, also eine jedermann grundsätzlich zugängliche.[79] Damit ist eine missbräuchliche Nutzung kaum wirksam verhindert.

(4) Übermaß an Grundrechtseingriffen/Totalüberwachung

Schließlich ist das RegMoG-E in der Gesamtschau der Maßnahmen der staatlichen Zugriffsrechte auf die Daten der Bürger zu betrachten. Das BVerfG hat in seiner Rechtsprechung immer wieder betont, dass die staatliche Datenverarbeitung nicht *auf eine Totalerfassung der Kommunikation oder Aktivitäten der Bürger insgesamt angelegt sein darf*;[80] *sie muss eine Ausnahme bleiben.*[81] Sie darf nicht einmal als Schritt hin zu einer Gesetzgebung verstanden werden, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte. Eine solche Gesetzgebung wäre, unabhängig von der Gestaltung der Verwendungsregelungen, von vornherein mit der Verfassung unvereinbar.[82] Es ist also die Gesamtbelastung der Bürger mit Informationseingriffen des Staates in den Blick zu nehmen, um zu verhindern, dass die gesamtheitliche Datenerfassung die Bürger nicht dem Eindruck einer Totalüberwachung aussetzt. Dies entspricht der ersten (!) Empfehlung der Datenethikkommission, nämlich Totalüberwachung zu verhindern[83] und den Rechtsrahmen risikoadäquat zu bestimmen[84]. Diesbezüglich erleichtert und in der Folge erweitert eine Identifikationsnummer, wie sie im RegMoG-E nach dem Gesetzeszweck vorgesehen ist, die Zugriffsmöglichkeiten der Verwaltung auf die beim Staat gespeicherten Datensätze der Bürger erheblich. Angesichts der ohnehin weitreichenden und in den letzten Jahren zunehmenden Möglichkeiten diverser Behörden, auf Daten von Bürgern zuzugreifen, ist eine solche weitreichende Verknüpfung nicht hinnehmbar.

(5) Once-Only und No-Stop-Government

Problematisch erscheint insoweit auch das Ziel des Gesetzgebers, mit Hilfe einer Identifikationsnummer Vorstellungen wie Once-Only und andere neuartige Verwaltungstätigkeiten ohne Einbindung der Bürger[85] umzusetzen, dafür aber Grundprinzipien des Datenschutzes in Frage zu stellen.

Once-Only steht für ein Leitbild aus der Europäischen Union, demnach Bürger ihre Daten der gesamten Verwaltung nur noch ein einziges Mal mitteilen sollen. Die Verwaltung muss von sich aus in der Lage sein, diese Daten, etwa aus einem übergreifenden Stammdatenregister oder aus dem jeweiligen bereichsspezifischen Register, abzurufen. Damit wird die Idee der Datensparsamkeit aufgegriffen und die Zweckbindung der erfassten Daten gelöst. In der Folge wird der Komfort einer einmaligen Dateneingabe im Kontakt mit der Verwaltung zum Abwägungsinteresse gegenüber den Interessen des Bürgers, nicht ausgeforscht und dem Staat aus¬geliefert zu sein. Dies kann angesichts der erheblichen Grundrechtseingriffe kein überwiegender Belang sein, zumal der Bürger nur in einzelnen Bereichen in häufigem oder regelmäßigem Kontakt mit Behörden steht, der Komfortgewinn also gering ist und vor allem auch durch andere Mittel erzielt werden kann.[86] Once-Only-by-default verstößt ohnehin gegen die bisherigen Datenschutzbestimmungen.[87]

No-Stop-Government steht für ein Leitbild von Verwaltung, bei dem die Bürger die Verwaltung nicht mehr spüren oder wahrnehmen und Behörden von sich aus für den Bürger aktiv werden. Bürger könnten, aber müssten Anträge nicht mehr selbst stellen. Technisch würde damit auf Kundenbeziehungsmanagementsysteme quer über den gesamten öffent-lichen Sektor gesetzt, die Zugriff auf alle relevanten Datenbestände erhalten, den künftigen Bedarf eines Bürgers von sich aus erkennen und proaktiv tätig werden. Die Grundüberlegung des Rechtsstaats und der Demokratie, dem Bürger eine umfängliche Kontrolle über „seinen" Staat zu ermöglichen, wäre damit ad absurdum geführt, bis hin dazu, dass die Technikkonzerne, die solche Konzepte bereitstellten, mit ihren normativen Vorstellungen Staatlichkeit bestimmten und nicht ein gewaltenteilender Staat mit einer Letztverantwortung gegenüber dem Bürger und Gerichten.

Die Einführung der Identifikationsnummer ist ein wesentlicher Schritt auf diesem Wege der Zusammenführung der Daten. Welche Mächtigkeit für den Staat und die zugrundeliegende, möglicherweise von privater Seite betriebene Infrastruktur dadurch entsteht, wird daran sichtbar, dass heutige IT-Systeme innerhalb kürzester Zeit (in Sekundenschnelle bei Nutzung der Datenverarbeitungskapazitäten eines durchschnittlichen Laptops) die Daten von mehr als 83 Millionen Bürgern und Steuerpflichtigen aus mindestens 56 Registern verknüpfen und auswerten können. Sind die Daten einmal zusammengeführt, lassen die Folgen sich nicht mehr beherrschen. Hier stellt sich die Frage, ob solche weitreichenden Vorstellungen zur Registermodernisierung überhaupt mit der Verfassung

[78] Vgl. BVerfGE 125, 260 (326 f.).
[81] *Wiss. Dienst BTag* 2020, Gutachten, S. 20.
[80] Vgl. BVerfGE 125, 260 (322 f.) und die – im Zuge der Umorganisation der BfDI – erfolgte Stellungnahme der BfDI, https://www.bundestag.de/blob/344116/3259a3ff-471bfda524b8ae4138e63f77/vosshoff-data.pdf.
[81] Vgl. BVerfGE 125, 260 (324).
[82] Vgl. BVerfGE 125, 260 (323).
[83] *Datenethikkommission* 2019, S. 18 und S. 89.
[84] *Datenethikkommission* 2019, S. 18 und S. 96 ff.
[85] Vgl. *Stocksmeier/Hunnius* 2018, S. 262 f.
[86] Siehe gleich unten Teil D.V.
[87] Unterkomplex *Martini/Wenzel*, DVBl. 2017, 749, der vor allem die Kosteneinsparungen und Effizienzgewinne und nicht die Bürgerrechte in den Vordergrund rückt (Fn. 6).

und den europäischen Datenschutzanforderungen in Übereinklang bringen lassen, wenn die eigentlichen Ziele der Politik Machine-2-Machine (Government), Once Only, No Stop Government oder No Government sein sollten.[88]

4. Verstoß gegen Gleichheitsgrundsätze und Art. 12 und 14 GG

Die Anknüpfung der Identifikationsnummer an die Steuer-ID nach § 139b AO behandelt natürliche Personen unabhängig von ihrer Funktion im Steuerverfahren gleich. Es wird nicht zwischen ihrer Rolle als „Privatperson" oder ihrer Rolle als „verantwortlich Handelnde im Wirtschaftsverkehr" beziehungsweise als „Einzelunternehmer oder freiberuflich Tätiger" unterschieden, obwohl unterschiedliche Anlässe für die Erfassung gegeben sind. Personen, die also gleichzeitig auch in anderer Funktion von § 139b AO erfasst sind, werden daher zusätzlich und ohne Differenzierung identisch mit natürlichen Personen behandelt. Eine eineindeutige Identifikation von Personengesellschaften als eigenständiges Rechtssubjekt, von juristischen Personen und von sonstigen Organisationen fehlt.[89]

IV. Europarecht

Auch unter europarechtlichen Gesichtspunkten stößt das RegMoG-E auf erhebliche Bedenken, sowohl aus primär- (Art. 7 und Art. 8 EU-GRCh) als auch sekundärrechtlichen Erwägungen (DSGVO).

1. Primärrecht

Das Datenschutzrecht wird von Art. 7 und Art. 8 GR-Ch geschützt; beide Grundrechte stehen in einem „engen Zusammenhang"[90] mit sich überschneidenden Schutzbereichen.[91] Bezüglich der Eingriffsintensität und der Verhältnismäßigkeit zeigen sich bisher zum Verständnis des BVerfGs erhebliche Überschneidungen, bis hin dazu, dass in den jüngeren Entscheidungen zur Vorratsdatenspeicherung eine Verschärfung offenbar wurde[92]. Daher kann insgesamt davon ausgegangen werden, dass die obigen Bedenken aus dem nationalen Verfassungsrecht in ähnlicher Weise auch der Wertung des EU-Primärrechts entsprechen. Dies gilt insbesondere für die weitreichende Verknüpfung und die mangelnde Bestimmtheit und Zweckbeschränkung.

2. Sekundärrecht (DSGVO)

Spezielle Ausprägung hat der Datenschutz in der EU mit der DSGVO gefunden. Diese ist anwendbar,[93] wenngleich die Öffnungsklauseln des Art. 6 Abs. 2 und Abs. 3 dem nationalen Gesetzgeber weite Gestaltungsspielräume einräumen.[94]

a) Art. 87 DSGVO

Die DSGVO sieht grundsätzlich die Einführung einer sog. Nationalen Kennziffer oder anderer Kennzeichen von allgemeiner Bedeutung in Art. 87 S. 1 DSGVO vor und trifft Regelungen dazu. Die Mitgliedstaaten können die spezifischen Bedingungen einer Verarbeitung dieser Kennziffer selbst bestimmen. Es handelt sich bei der Regelung um eine optionale Öffnungsklausel.[95]

(1) Nationale Kennziffer oder Kennzeichen von allgemeiner Bedeutung

Eine Legaldefinition für die Begriffe der nationalen Kennziffer und der anderen Kennzeichen von allgemeiner Bedeutung sieht die DSGVO nicht vor. Die Literatur versteht unter dem Begriff der nationalen Kennziffer eine in der Regel staatlich zugeteilte Zeichenkette, die jeweils eindeutig einen bestimmten Bürger oder Einwohner identifiziert und die umfassend oder zumindest für mehrere definierte Sektoren oder Lebensbereiche verwendet wird.[96] Wann ein anderes Kennzeichen allgemeine Bedeutung erlangt, ist nicht abschließend geklärt. Es handelt sich bei der nationalen Kennziffer jedenfalls um einen Unterfall eines Kennzeichens allgemeiner Bedeutung.[97]

Ob die Steuer-ID nach § 139a AO bereits in gegenwärtiger Form unter die Regelung des Art. 87 DSGVO fällt, ist umstritten; eine wohl knappe Mehrheit in der Literatur bejaht dies.[98] Die Gegenauffassung vertritt hingegen zumeist das Argument, dass eine „allgemeine Bedeutung" bei bereichsspezifischen Kennzeichen nicht vorliegen kann.[99] Durch die Ausweitung der Identifikationsnummer auf 56 weitere Register im Rahmen des RegMoG-E, die alleine durch die Zuordnung auch dem Anwendungsbereich der DSGVO unterliegen, wird jedoch auch nach der Gegenauffassung jedenfalls von einem Kennzeichen von allgemeiner Bedeutung auszugehen sein.[100] Davon geht auch die Begründung des RegMoG-E aus, wonach der Gesetzentwurf von der Öffnungsklausel des Art. 87 S. 1 DSGVO ausdrücklich Gebrauch macht.[101]

[88] Siehe dazu z.B. die Entscheidung und Empfehlung des IT-Planungsrats, https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/26_Sitzung/TOP2_Anlage_OZGUmsetzungskatalog.pdf?__blob=publicationFile&v=4 (Stand 4/2018), S. 263 ff.
[89] *BRat* 2020, S.4
[90] EuGH Rs. C-92/09 und C-93/09, EuZW 2010, 939 Rn. 47.
[91] EuGH Rs. C-92/09 und C-93/09, EuZW 2010, 939 Rn. 52.
[92] Vgl. *Schiedermair*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Einleitung, Rn.173.
[93] Siehe oben unter Anwendung der DSGVO und rechtlicher Prüfungsmaßstab.
[94] Siehe oben unter Anwendung der DSGVO und rechtlicher Prüfungsmaßstab.
[95] *Hansen* 2019, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 8.
[96] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 12.
[97] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 12.
[98] *Ehmann*, in: Ehmann/Selmayr 2018, Art. 87, Rn. 7; *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 14; *Pauly*, in: Paal/Pauly 2019, Art. 87 DSGVO Rn. 2; *Gola*, in: Gola 2018, Art. 87.
[99] *von Lewinski*, in: BeckOK 2020, Art. 87 Rn. 53; wohl auch Weichert, in: Kühling/Buchner 2020, Art. 87 Rn. 22; *Martini/Wagner/Wenzel* 2017, S. 5.
[100] *Wiss. Dienst BTag* 2020, Gutachten, S. 6 f. mit Hinweis auf die Existenz von insgesamt 214 Registern in Deutschland.
[101] RegMoG-E, S. 40.

(2) Grenzen der Öffnungsklausel: Geeignete Garantien

Art. 87 S. 2 DSGVO schreibt vor, dass die Mitgliedstaaten im Falle einer Einführung eines entsprechenden Kennzeichens geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen festlegen müssen. Hiervon umfasst sind gesetzliche, technische und organisatorische Maßnahmen.[102] Aus dieser Formulierung ergeben sich Mindestanforderungen, die erfüllt sein müssen; die Vorgaben der DSGVO sind im Prinzip einzuhalten und die Prüfung des notwendigen Schutzniveaus geboten. Dies ist für den gesamten Lebenszyklus der Kennungen und der Verarbeitung zu gewährleisten.[103] Zu solchen geeigneten Garantien gehören enge Zweckbindung, Verwendungs- und Weitergabebeschränkungen, Begrenzung der Form der Verarbeitung, die Ausgestaltung des Kennzeichens, frühestmögliche Pseudonymisierung und Umkodierungen, Schutz vor Täuschung und Manipulation sowie ausreichender Rechtsschutz einschließlich Sanktionstatbeständen.[104] Es müssen die wesentlichen Elemente des Schutzniveaus der DSGVO, und damit die wesentlichen Prinzi-pien aus Art. 5 DSGVO[105] und seiner Konkretisierungen wie z.B. die besonderen Anforderungen des Art. 32 DSGVO, gewahrt bleiben, nämlich enge Zweckbindung, Vorhersehbarkeit, Datenminimierung, Speicherbegrenzung, Rechtmäßigkeit einschließlich Bestimmbarkeit, Richtigkeit, Transparenz und Rechenschaftspflicht. Der gänzliche Verzicht auf einzelne Prinzipien ist damit ebenso wenig vereinbar wie eine deutliche Reduktion der meisten dieser Garantien.

Schon deshalb mit der DSGVO nicht vereinbar ist die Einzelansicht, der Grundsatz der Zweckbindung sei nicht von den Garantien iSd. Art. 87 S. 2 DSGVO erfasst, weil das Ver-knüpfungspotential eines solchen Kennzeichens die allgemeine Wiederverwendbarkeit voraussetze.[106] Dieser Zirkelschluss von der möglichst breit gewünschten Verwendungsmöglichkeit auf die Verwendungszulässigkeit wird auch in anderen Bereichen der DSGVO nicht mitgegangen, zum Beispiel beim Profiling: Aus dem unbegrenzten technischen Können folgt gerade kein unbegrenztes normatives Dürfen. Es ist auch nicht erkennbar, dass die Begrifflichkeit der Garantien in Art. 87 S. 2 DSGVO anders zu verstehen wäre als in anderen Vorschriften in der DSGVO, etwa in Art. 6 Abs. 4 lit. e) DSGVO.[107] Die Vorschrift baut auf einer Vorgängervorschrift in der DS-RL auf und soll den Mitgliedstaaten ermöglichen, bestehende Kennzeichen fortzuführen.[108]

Auch wenn die vorgesehene Identifikationsnummer eine Reihe von gebotenen Sicherungen und Garantien enthält, sind diese dennoch nicht ausreichend. Denn die Zweckbindung wird faktisch unterlaufen, indem eine Vielzahl von Registern verknüpft wird; die technischorganisatorischen Sicherungen werden nicht konkretisiert und vorgegeben; der Überwachungsdruck wächst dadurch in unangemessener Weise. Auf die angesprochenen Grundrechtsverkürzungen kann verwiesen werden.[109]

b) Art. 6 Abs. 1 lit. e) i.V.m. Art. 6 Abs. 2 und Abs. 3 DSGVO

Fraglich ist, ob parallel zu Art. 87 DSGVO auch die Vorschrift des Art. 6 Abs. 1 lit. e) DSGVO i.V.m. Art. 6 Abs. 2 und Abs. 3 DSGVO zu beachten ist. Sie ermöglicht den Mitgliedstaaten, eigene Regelungen für die Legitimation von Datenverarbeitungen – also auch Zuweisungen von Identifikationsnummern – im öffentlichen Interesse – also für Verwaltungszwecke – vorzunehmen.

(1) Verhältnis zwischen Art. 87 und Art. 6 DSGVO

Art. 6 Abs. 1 lit. e) DSGVO deckt bereits nach seinem Wortlaut einen deutlich weiteren Raum ab als Art. 87 DSGVO. Zweck des Art. 87 DSGVO ist insofern die Klarstellung, dass der Gesetzgeber Personenkennzeichen grundsätzlich einführen kann.[110] Aufgrund der für solche Kennzeichen typischen Risiken bestünde anderenfalls die Möglichkeit, dass Zweifel an deren Rechtmäßigkeit aufträten.[111] Das dogmatische Verhältnis zwischen Art. 87 DSGVO und Art. 6 DSGVO ist jedoch nicht eindeutig.

Nach dem Wortlaut sieht Art. 87 S. 1 DSGVO nur spezifische Regelungen für die Verarbeitung des Kennzeichens als solches vor. Hiervon umfasst sind alle Verarbeitungsvorgänge im Sinne von Art. 4 Nr. 2 DSGVO, also auch die Erschaffung und Übertragung des Kennzeichens. Ob dies jedoch auch auf jene Daten zutrifft, die im Rahmen des IDNrG-E zusammen mit der Identifikationsnummer abgefragt und übermittelt werden, ist fraglich. So vertritt eine Ansicht, dass Art. 87 S. 1 DSGVO die Schaffung einer Rechtsgrundlage für die Zuteilung des Kennzeichens und die hierfür erforderlichen Stammdaten ermöglicht.[112] Die Übermittlung von Daten, die mit dem Kennzeichen verbunden sind, können hiernach jedoch nicht auf die Regelung in Art. 87 S. 1 DSGVO gestützt werden.[113]

Art. 87 S. 1 DSGVO enthält keinen eigenen Erlaubnistatbestand für Verarbeitungen unter Verwendung eines solchen Kennzeichens.[114] Die Vorschrift stellt vielmehr eine Angemessenheitsregelung auf.[115] Eine entsprechende Verarbeitung muss demnach bereits nach den Art. 6 und 9 DSGVO zulässig sein.[116] Die Erlaubnistatbestände in Art. 6 DSGVO sind nach der Systematik der DSGVO grundsätzlich als abschließend einzustufen.[117] Diese Auslegung wird darüber hinaus dem Zweck von Art. 87 DSGVO gerecht, die grundsätzliche Zulässigkeit von Kennzeichen zu betonen.

[102] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 23.
[103] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 24 f.
[104] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 26 ff.
[105] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 25.
[106] *Von Lewinski*, in: BeckOK 2020, Art. 87 Rn. 45.
[107] Auch hier sind alle Grundsätze des Art. 5 DSGVO zu wahren: *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 6 Abs. 4 Rn. 65.
[108] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 2.
[109] Siehe oben unter Angemessenheit.
[110] *Ehmann*, in: Ehmann/Selmayr 2018, Art. 87 Rn. 1; *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87 Rn. 1.
[111] *Ehmann*, in: Ehmann/Selmayr 2018, Art. 87 Rn. 1; Hansen, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87 Rn. 9.
[112] *Martini/Wagner/Wenzel* 2017, S. 8 mit dem Hinweis, dass bei anderweitiger Ansicht Art. 6 Abs. 3 S. 1 DSGVO als einschlägig zu betrachten sei.
[113] *Martini/Wagner/Wenzel* 2017, S. 11,
[114] *Ehmann*, in: Ehmann/Selmayr 2018, Art. 87 Rn. 11; *Weichert*, in: Kühling/Buchner 2020, Art. 87 Rn. 4
[115] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 8.
[116] *Ehmann*, in: Ehmann/Selmayr 2018, Art. 87 Rn. 11; Weichert, in: Kühling/Buchner 2020, Art. 87 Rn. 4.
[117] *Schulz*, in: Gola 2018, Art. 6 Rn. 9.

Welche Ansicht die Bundesregierung in dieser Frage vertritt, lässt sich der Begründung des Entwurfs nicht unmittelbar entnehmen; ausdrücklich wird das RegMoG-E auf Art. 87 DSGVO gestützt[118]. Die vorhandenen Ausführungen zu Art. 6 DSGVO beschränken sich jedoch auf pauschale Hinweise zur Rechtmäßigkeit der Datenverarbeitung bei Übertragung von Daten nach § 6 III IDNrG-E.[119] Der Gesetzentwurf muss allerdings auch die Voraussetzungen des Art. 6 DSGVO neben Art. 87 DSGVO einhalten.

(2) Voraussetzungen von Art. 6 Abs. 3 DSGVO

Art. 6 Abs. 1 lit. e) DSGVO ist – im Gegensatz zu den meisten anderen in Art. 6 Abs. 1 DSGVO aufgeführten Alternativen – kein eigenständiger Erlaubnistatbestand.[120] Vielmehr dient die Norm im Zusammenspiel mit Art. 6 Abs. 3 DSGVO als „Scharnier"; der eigentliche Erlaubnistatbestand ist in dem vom Mitgliedstaat erlassenen Recht zu sehen.[121] Abs. 2 ist als weiter denn Abs. 3 zu verstehen; Abs. 3 betrifft nur die Zulässigkeit der Datenverarbeitung i.V.m. Art. 6 Abs. 1 lit. c) und lit. e) DSGVO sowie benennt in Abs. 3 S. 2 weiterreichende Angaben im Zusammenhang mit der Rechtsgrundlage.[122] Die Vorschriften des RegMoG-E schaffen eine Rechtsgrundlage für die Verarbeitung von Daten auf der Basis des Art. 6 Abs. 1 lit. e) DSGVO, so dass zunächst Abs. 3 vorrangig den Prüfungsmaßstab vorgibt.

Demnach sind „spezifische Bestimmungen" im mitgliedstaatlichen Recht zulässig, welche die Umsetzung der Grundsätze der Datenverarbeitung in Art. 5 DSGVO konkretisieren[123] und zu kohärenten Gesamtregelungen beitragen, welche die Risikosituation einer bestimmten Form der Datenverarbeitung umfassend regeln[124].

Dem Gesetzgeber ist also nicht verwehrt, z.B. einheitliche Regelungen für die Verwendungen bereichsspezifischer Personenkennziffern zu schaffen. Gleichwohl stellen weder Abs. 2 noch Abs. 3 Regelungen dar, die ein grundsätzliches Abweichen von den Prinzipien der DSGVO erlaubten. Daher gilt auch hier, dass die nicht vereinbaren Regelungen des RegMoG-E nicht über Art. 6 Abs. 2 bzw. Abs. 3 DSGVO legitimiert werden können.

c) Zu berücksichtigende Prinzipien, insb. Art. 5 DSGVO

Ohnehin ist zu berücksichtigen, dass die Nutzung einer Öffnungsklausel, also auch von Art. 87 DSGVO, nicht von den Bindungen der DSGVO gänzlich freistellt, sondern weiterhin grundsätzlich alle Vorgaben der DSGVO umzusetzen sind.[125] Insbesondere eine Berücksichtigung der Grundsätze des Art. 5 DSGVO ist notwendig.[126]

(1) Datenminimierung

Der Grundsatz der Datenminimierung nach Art. 5 Abs. 1 c) DSGVO gebietet es, personenbezogene Daten auf das für die Zwecke der Verarbeitung notwendige Maß zu begrenzen. Die Erhebung des letzten Verwaltungskontakts nach § 4 Abs. 3 Nr. 2 IDNrG-E als „Lebenszeichen"[127] einer natürlichen Person ist insofern für die Zwecke des Gesetzes, ein registerübergreifendes Identitätsmanagement zu schaffen und damit Redundanzen zu verringern, verfehlt.[128] Hier besteht die Gefahr eines übergreifenden Tracings von Bürgern; um die Datenqualität durch die Validitätswerte festzustellen, genügt laut der *Gesellschaft für Informatik* insoweit auch das Datum der letzten Aktualisierung der Validitätswerte.[129]

Ähnliches gilt für die Form der Übertragung der Daten bei der Abfrage durch Behörden. Soll etwa festgestellt werden, dass es sich vorliegend um einen deutschen bzw. EU-Staatsbürger handelt (vgl. das Basisdatum „Staatsangehörigkeiten" in § 4 Abs. 2 Nr. 8 IDNrG-E), reicht regelmäßig bereits die bejahende oder verneinende Beantwortung dieser Frage.[130]

Daneben besteht die Gefahr, dass Register Daten erhalten bzw. die Identifikationsnummer hinzufügen sollen, die keine Verwendung dafür haben. So kritisiert die Bundesrechtsanwaltskammer (BRAK), dass im Gesamtverzeichnis bei der BRAK (IDNrG-E Anlage Nr. 46) lediglich Namen und Doktorgrad eingetragen seien und keinerlei Verwaltungsleistungen erbracht würden.[131] Die in der Anlage des IDNrG-E genannten Register bedürfen somit zumindest einer weiteren Überprüfung.

(2) Zweckbindung

Personenbezogene Daten müssen gemäß Art. 5 Abs. 1 b) DSGVO für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden. Ein eindeutiger Zweck ist von anderen möglichen Zwecken klar zu unterscheiden; er muss ausdrücklich benannt, inhaltlich präzise und konkret bestimmt sein.[132] Die Art. 29 Working Party erachtet vor diesem Hintergrund pauschale Zweckbestimmungen wie „Verbesserungen der Nutzererfahrung", „Marketing", „IT-Sicherheit" und

[118] RegMoG-E, S. 72.
[119] Vgl. RegMoG-E, S. 80
[120] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 6 Abs. 1, Rn. 71.
[121] *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 6 Abs. 1, Rn. 71.
[122] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 6 Abs. 2, Rn. 7.
[123] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 6 Abs. 3, Rn. 38.
[124] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 6 Abs. 3, Rn. 38; ders., DuD 2018, 477.
[125] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 24; punktuelle Abweichungen erlaubend: *Ehmann*, in: Ehmann/Selmayr 2018, Art. 87 Rn. 9; einen zumindest, der DSGVO gleichwertigen Mindestschutz fordert *Pauly*, in: Paal/Pauly 2019, Art. 87, Rn. 3; a.A. *von Lewinski*, in: BeckOK 2020, Art. 87, Rn. 44, der nur einzelne Grundsätze der DSGVO für anwendbar hält.
[126] *Martini/Wagner/Wenzel* 2017, S. 7; vgl. Forderungen hinsichtlich Transparenz und Zweckbindung bei *Pauly*, in: Paal/Pauly 2019, Art. 87 Rn. 3 und *Weichert*, in: Kühling/Buchner 2020, Art. 87 Rn. 15.
[127] So RegMoG-E, S. 77.
[128] Mit Verweis auf das Prinzip der Datensparsamkeit vgl. auch GI 2020, S. 6.
[129] *GI* 2020, S. 6.
[130] Vgl. *Martini/Wagner/Wenzel* 2017, S. 10.
[131] BRAK, S. 2 f. Der RegMoG-E nennt nach Kritik an der Verwendung des Begriffs „Anwaltsverzeichnis" im Referentenentwurf nun ausdrücklich die Verzeichnisse der Rechtsanwaltskammern und das Gesamtverzeichnis der BRAK.
[132] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 5 Rn. 76.

„zukünftige Forschung" für nicht ausreichend.[133] Grundsätzlich gilt, dass der Zweck desto bestimmter festgelegt sein muss, je eingriffsintensiver eine Maßnahme ist.[134]

Dem Gesetzentwurf gelingt keine klare Zweckbestimmung. § 1 IDNrG-E schreibt zunächst verschiedene Ziele des Gesetzes fest; in § 5 IDNrG-E wird sodann ausdrücklich der Zweck der Identifikationsnummer bestimmt. Während die Zweckbestimmung in § 5 Abs. 1 Nr. 1 und 2 IDNrG-E („Zuordnung der Datensätze zu einer Person" und „Abgleich von Datensätzen einer natürlichen Person […]") noch als ausreichend bestimmt angesehen werden kann, gilt dies nicht für § 1 IDNrG-E. Die Verbesserung der Datenqualität wird in der Gesetzes-begründung zwar als einer der Zwecke der Datenverarbeitungen genannt (bspw. für die Erhebung des Datums des letzten Verwaltungskontakts); ist jedoch nur eines der Ziele in § 1 IDNrG-E. Es ist auch unklar, inwieweit dies in Bezug auf alle 56 Register erreicht wird und nicht vielmehr eine pauschale Zusammenfassung darstellt. Die Eingrenzungsfunktion, die über die Zweckbestimmtheit erreicht werden soll, ist kaum gewahrt; für Bürger ist kaum erkennbar, wer Zugriff auf die Identifikationsnummer und die damit verbundenen Informationen haben kann, soll und darf. Insoweit § 1 IDNrG-E auch als Zweckbestimmung dienen soll, ist dies inhaltlich nicht ausreichend präzise dargestellt, erst recht nicht, wenn man die Gefahr der Profilbildung und der Verstärkung der Machtasymmetrie zu Lasten der Bürger als eingriffsintensiv ansieht. Gerade diese Wertung ist der DSGVO jedoch zu entnehmen.[135]

Letztlich besteht mit dem Entwurf die Gefahr, dass neben der ohnehin schon breiten Zweckbestimmung umfangreiche Zweckänderungen unter den allgemeinen Regelungen der Art. 5 Abs. 1 lit. b) und Art. 6 Abs. 4 DSGVO möglich werden.[136] Vor diesem Hintergrund schlägt der BfDI vor, der Identifikationsnummer mit der Identifikation von natürlichen Personen gegenüber der Verwaltung einen einzigen Zweck zuzuordnen.[137] Ferner wäre ein ausdrücklicher Hinweis, dass die Identifikationsnummer auch nur zu diesem Zweck verarbeitet werden darf, zu begrüßen.[138]

(3) Transparenz

Art. 5 Abs. 1 lit. a) Alt. 3 DSGVO sieht vor, dass personenbezogene Daten in einer für die betroffenen Person nachvollziehbaren Weise verarbeitet werden müssen. Das RegMoG-E schafft mit der Einführung des Datencockpits nach § 10 OZG-E einen Mechanismus, der dem Bürger veranschaulicht, welche Datenverarbeitungen die Verwaltung im Zusammenhang mit der Identifikationsnummer durchführt. Als Reaktion auf Kritik des BfDI[139] wurde in § 10 Abs. 2 S. 2 2. HS und S. 3 OZG-E eine Regelung geschaffen, die die Aufbewahrung der Daten auf die Dauer der jeweiligen Nutzersession begrenzt.

Sollte sich das Datencockpit als Mittel zur Vermittlung von Transparenz bei der Datenverarbeitung durch Behörden bewähren, könnte der Gesetzgeber eine Erweiterung des Datencockpits auch auf andere Verwaltungsbereiche in Betracht ziehen.[140]

(4) Datenqualität und -richtigkeit

Personenbezogene Daten müssen schließlich gemäß Art. 5 Abs. 1 lit. d) DSGVO sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Die Datenqualität ist zwar eines der Ziele des Gesetzentwurfs. Die Erreichung dieses Ziels durch das RegMoG ist fraglich. Vielmehr wird von den einzelnen Fachbehörden verlangt, ihrerseits geprüfte Daten mit Daten unbekannter Qualität zu ersetzen, sodass es auch zu einer Verschlechterung der Datenqualität kommen kann.[141] Ebenso wenig ist eindeutig geregelt, welche Behörde für die Richtigkeit der Daten zuständig ist und wie mit potentiellen Dubletten umgegangen werden soll.[142] Diesbezüglich fehlt es also auch an der Bestimmtheit der Vorgaben.

V. Zwischenfazit

Dem RegMoG-E und insbesondere dem IDNrG-E stehen in ihrer aktuellen Form erhebliche verfassungsrechtliche und europarechtliche Bedenken entgegen. Zwar ist die Einführung eines Datenschutzcockpits im OZG-E grundsätzlich als Transparenzmaßnahme gegenüber den Bürgern zu begrüßen. Transparenz alleine vermag jedoch nicht die Intensität des Eingriffs durch die bereichsübergreifende Identifikationsnummer auszugleichen, zumal diese Transparenz nur zu einem nachgelagerten Rechtsschutz befähigt. Hier sind weitere Schutzmaßnahmen gefragt, um der Rechtsprechung des BVerfGs in der Folge des Volkszählungsurteils und den Vorstellungen des europäischen Gesetzgebers zur DSGVO ausreichend Rechnung zu tragen.

Besonders bedenklich ist die Tatsache, dass das BMI laut eigener Gesetzesbegründung weitere Datenschutzmaßnahmen pauschal aus Kosten- und Zeitgründen ablehnt.[143] Die deutsche Verwaltung bedarf zweifellos einer Modernisierung, um Redundanzen zu verringern und die Effizienz zu steigern; in Zeiten von verstärkter digitaler Kommunikation durch Covid-19 gilt dies erst recht. Mit dem österreichischen Modell gibt es auf europäischer Ebene jedoch bereits eine funktionsfähige Variante eines digitalen Identitätsmanagements, die – auch bei einiger berechtigter Kritik an diesem Modell[144] – deutlich datenschutzfreundlicher gestaltet ist als der aktuelle nationale Gesetzesentwurf. Insofern wird vom Gesetzgeber nicht erwartet, das Rad sprichwörtlich „neu zu erfinden" oder eine ähnliche Kraftanstrengung wie zur Etablierung der Corona-App zu stemmen. Darüber hinaus sendet der Staat

[133] Art. 29 Working Party, S. 16.
[134] Vgl. *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 5 Rn. 69 ff.
[135] So etwa in Art. 35 Abs. 3 lit. a), siehe hierzu auch *Karg*, in Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 35, Rn. 37 ff.
[136] *BfDI* 2020, S. 9.
[137] *BfDI* 2020, S. 9.
[138] So auch die *DRV* 2020, S. 10.
[139] *BfDI* 2020, S. 10.
[140] So auch gefordert von dem *BfDI*, S. 10 und BDA, S. 2.
[141] *Databund*2020, S. 2.
[142] *Databund* 2020, S. 2.
[143] RegMoG-E, S. 3.
[144] Siehe noch unten Teil D.

ein falsches Signal, die ursprünglich nur für die Steuerverwaltung angedachte Identifikationsnummer nunmehr nachträglich auf alle Lebensbereiche auszuweiten. Eine solche Funktionsexplosion („function creep“) hat das Potential, das Vertrauen in den Gesetzgeber zu erschüttern und sollte daher möglichst verhindert werden.

Abb. 5 | Morphologischer Kasten zum Identitätsnummernsystem RegMoG

ID-NR-SYSTEM	AUSPRÄGUNGSFORMEN				
Typus von Personenkennzeichen	**allgemeines Personenkennzeichen (aPK)**	bereichsübergreifendes Personenkennzeichen (2wPK)	bereichsspezifisches Personenkennzeichen (bPK)		
Vorgehen bei der Vergabe	**Personenkennzeichen zentral vergeben**		Personenkennzeichen dezentral vergeben		
Inhaltliche Gestaltung des Personenkennzeichens	**Steuer-ID**	Andere existierende Register-ID	NEU-ID/Stammzahl in Form von einer Zufallszahl	Keine zentrale ID	
Identifizierung in anderen Registern	**Steuer-ID**	Bisherige Register-ID	Hashwert auf Stammzahl und Bereichs-Bezeichner	Zufallszahl	
Zu erfassende Personengruppe	**Deutsche Bürger**	**Ausländer**	**Steuerzahler**	**Natürliche Personen**	Juristische Personen
Verortung der Speicherung der Basisdatensätze zu allen Personen	**Basisdatensatz beim Bundeszentralamt für Steuern (BZSt)**		ohne Basisdatensatz		
Einsatz einer Intermediär-internen Datenbank mit allen bPKs	**Verzicht auf Intermediär-interne ID-Datenbank**		Pseudonymisierte Intermediär-interne ID-Datenbank		
Registermodernisierung	**Registermodernisierungsbehörde (BVA)**		Verzicht auf Registermodernisierungsbehörde		
Verortung der Intermediäre zu den BZSt-Basisdatensätzen	**Intermediär zum BZSt-Basisdatensatz bei BVA (Registermodernisierungsbehörde)**		Intermediär zum BZSt-Basisdatensatz bei Datenschutzaufsichtsbehörde		
Vermittlungsstellen für Anfragen auf BZSt-Basisdatensätze	Keine Vermittlungsstelle für Anfragen	**Zentrale Vermittlungsstelle für Anfragen**	Verbund von Vermittlungsstellen für Anfragen		
Prüfung der Zugriffe auf BZSt-Basisdatensätze	Keinerlei Prüfung der Zugriffe	**Software-basierte Prüfung der Zugriffe**	Hardware-basierte Prüfung der Zugriffe	Ständige Prüfung durch Sachbearbeiter	
Freigabe von Daten durch Bürger bei bereichsübergreifenden Abfragen	**Freigabe von Daten ohne Bürgereinbindung**	Anlassbezogene Freigabe von Daten durch Bürger	Freigaben von Daten stets durch Bürger erforderlich		

Das RegMoG-E führt also zu einem Identitätsnummernsystem (**Abbildung 5**), das mit der Steuer-ID auf einem allgemeinen Personenkennzeichen aufsetzt, das vom Bundeszentralamt für Steuern zentral vergeben und in allen relevanten Registern gespeichert wird. Zur eindeutigen Identifizierung von Personen in allen relevanten Registern reicht die Steuer-ID aus. Erfasst werden alle potentiellen Steuerzahler. Damit wird die gesamte Bevölkerung einbezogen. Beim Bundeszentralamt für Steuern werden Basisdaten gespeichert. Zugriffe auf diese Basisdaten und alle Anfragen erfolgen nur über die Registermodernisierungsbehörde. Eine separate ID-Datenbank bei Intermediären ist auf Grund dieser Konstellation nicht erforderlich. Alle Zugriffe werden automatisiert geprüft. Die Bürger selbst sind in diese Abfragen nicht eingebunden. Sie werden über das Datenkonto auf Zugriffe informiert.

Insgesamt hat damit das RegMoG-E die folgenden Konsequenzen,
die abschließend in einer SWOT-Analyse (**Abbildung 6**) zusammengefasst wurden:

Abb. 6 | SWOT-Analyse zum Identitätsnummernsystem RegMoG-E

STÄRKEN

- → Schneller und einfacher Zugriff der Verwaltung auf die bereichsspezifischen Datensätze
- → Verringerung der Zugangsbeschränkungen für nahtloses E-Government (Once-Only)
- → Existierende ID wird genutzt, Neuvergabeprozess entfällt
- → Steuer-ID als Anknüpfungspunkt betont die Bedeutung der Finanzverwaltung

SCHWÄCHEN

- → Gefahr des „gläsernen Bürgers“
- → Keine Beachtung der Vorgaben der Datenethikkommission
- → Alternativen werden unterkomplex betrachtet
- → Überbewertung der Bedeutung von Once-Only für die Bürger

CHANCEN

- → Erleichterter und künftig registerbasierter Zensus
- → Genauere Datenbestände
- → Missbrauch durch mehrere Identitäten parallel eingeschränkt
- → Einfachere Steuerung des Bürgers möglich

RISIKEN

- → Vorschnelles Agieren des Gesetzgebers und dadurch Nicht-Beachtung wesentlicher Problemlagen
- → Verstoß gegen nationale und europäische Grundrechte, insbesondere das Recht auf informationelle Selbstbestimmung
- → Überlagerung der inhaltlichen Fragen durch Konflikt des BVerfGs mit dem EuGH
- → Selbstbestimmung/Datenschutzgrundrecht
- → Verstoß gegen Bestimmtheits-anforderungen der Verfassung
- → Verstoß gegen das Demokratie- und Rechtsstaatsprinzip
- → Erschwernis für die Steuerverwaltung mangels Weiterverwendbarkeit der Steuer-ID.
- → Verstoß gegen den Gleichbehandlungsgrundsatz
- → Unpräzise, Art. 80 Abs. 1 S. 2 GG widersprechende Auslagerung von Entscheidungsspielräumen an die Verwaltung
- → Ermöglicht Profilbildung
- → Keine Beschränkung des Once-Only auf Bereiche, in denen regelmäßig und häufig Bürgerkontakte bestehen
- → Verlagerung der negativen Effekte von Bürokratie und fehlender Organisation in der Verwaltung auf den Bürger und dessen Freiheitsrechte
- → Missbrauchsgefahr einer Einzelidentität durch leichteren Identitätsdiebstahl (vgl. Social Security Number in den USA)

C. Drei Optionen: Kein neues Personenkennzeichen, ein neues allgemeines Personenkennzeichen oder ein neues bereichsspezifisches Personenkennzeichen

Mit Blick auf die erfolgte Bewertung des vorliegenden Gesetzesentwurfs stellt sich die Frage, welche Optionen es derzeit für die vom Normenkontrollrat eingeforderte und von der Bundesregierung und dem IT-Planungsrat forcierte Registermodernisierung noch gibt. Nüchtern betrachtet gibt es drei Optionen (**Abbildung 7**). Erstens kommt der Verzicht auf eine Einführung eines neuen Personenkennzeichens in Betracht. Ebenso wäre die Einführung eines neuen bereichsspezifischen Personenkennzeichens vorstellbar. Die dritte Option wäre die Einführung eines neuen allgemeinen Personenkennzeichens.

Abb. 7 | Optionen für Personenkennzeichen zur Registermodernisierung in Deutschland

Der Verzicht auf eine Einführung eines neuen Personenkennzeichens entspräche dem Status Quo. Dies verhindert zwar eine substantielle Registermodernisierung, setzt die Bevölkerung aber auch nicht den Gefahren, Risiken und Nebenwirkungen eines neuen Personenkennzeichens aus. Aus einer Datenschutzperspektive mag dieser Weg der Besitzstandswahrung große Unterstützung finden. Eine Registerkonsolidierung und modernisierung wäre aber nur mit hohem manuellem Aufwand möglich und würde auch die Umsetzung des OZG erschweren. Diese Option wird in diesem Gutachten nicht weiter verfolgt.

Mit dem RegMoG-E wird ein Vorschlag zur Einführung eines neuen allgemeinen Personenkennzeichens auf Basis der bisher bereichsspezifisch eingesetzten Steuer-ID eingebracht. Auf diesen Vorschlag, der zentral und registerübergreifend angelegt ist, wurde in der Analyse und Bewertung in Teil B bereits detailliert eingegangen. Die in diesem Zusammenhang ebenfalls denkbaren Alternativen einer neuartigen allgemeinen Identifikationsnummer ohne Rückgriff auf die Steuer-ID sowie auf Grundlage biometrischer Merkmale (wie dem Gesichtsprofil oder der Fingerabdrücke) werden nicht weiter verfolgt, weil sie ebenso nicht verfassungskonform wären und sich daher für einen Einsatz in der Bundesrepublik Deutschland generell nicht eignen.

Die Idee einer neuartigen bereichsspezifischen Identifikationsnummer, die ausschließlich zu Zwecken der Identifizierung von Personen im Rahmen von Registerzugriffen eingesetzt werden darf, ist eine überlegenswerte und ebenso rasch umsetzbare Alternative. Sichtbare Schwächen des vorliegenden Gesetzesentwurfs sind dabei beseitigt. Ausgangsbasis ist eine neuartige Identifikationsnummer (NEU-ID), die bisher noch keinerlei Verwendung findet. Andere Ansätze auf bestehenden bPKs wurden nicht weiter betrachtet, da diese dann zu aPKs würden und damit verworfen werden müssten. Dies hindert jedoch nicht daran, etwa die Gruppe aller Inhaber einer Steuer-ID als Ausgangsbasis für die Erzeugung neuer bPK zu verwenden.

In der folgenden Analyse in Kapitel D werden zwei machbare Varianten näher betrachtet, an denen die bestehenden Optionen verständlich aufgezeigt werden können.

→ **VARIANTE 1** (Stammzahl-Modell) greift mit einer geheim gehaltenen Stammzahl und daraus generierten Hash-werten als weiteren neuen bPK einige Ideen aus Österreich auf. Nur die Registermodernisierungsbehörde (BVA) kennt und verwendet die Stammzahlen. Auf Basis der Stammzahl und eines Bezeichners pro Register generiert sie nach österreichischem Vorbild alle hash-basierten bPKs. Anschließend übermittelt sie diese zur ausschließlich lokalen Speicherung an die jeweiligen Register. Auf eine Speicherung aller Personenkennzeichen in einer eigenständigen ID-Datenbank wird vollkommen verzichtet. Die Basisdaten verbleiben beim Bundeszentralamt für Steuern. Die Registermodernisierungsbehörde kann eine Registerkonsolidierung initiieren, indem sie zu jeder Person die jeweiligen Basisdaten bei allen Registern abfragt, diese dann qualitätssichert und an die bereichsspezifischen Register zurückspielt. Alle anderen Anfragen laufen über Vermittlungsstellen und die Registermodernisierungsbehörde. Behörden untereinander sind nicht in der Lage, aus ihren jeweiligen bereichsspezifischen Identifikationsnummern heraus alle Daten zu einer Person zusammenzuführen.

→ **VARIANTE 2** (NEU-ID-Modell) setzt auf eine neuartige bereichsspezifische NEU-ID und eine neue, zentrale und besonders geschützte ID-Datenbank bei einer Datenaufsichtsbehörde, etwa dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. In diesem neuen pseudonymisierten Register werden zu jeder Person alle bestehenden bPKs oder weitere neu zu generierende bPKs gespeichert, aber keinerlei Basisdaten. Die Basisdaten verbleiben weiterhin beim Bundeszentralamt für Steuern. Die Registermodernisierungsbehörde (BVA) übernimmt die Aufgaben der Registermodernisierung. Alle Anfragen laufen über Intermediäre (wie die Vermittlungsstellen). Die bereichsspezifische Identifikationsnummer NEU-ID muss für den gesamten Personenkreis neu vergeben werden. Sie wird aber nur innerhalb dieser ID-Datenbank verwendet. Der Aufbau und der dauerhafte Schutz einer solchen ID-Datenbank wird sich datenschutzrechtlich als Herausforderung erweisen, erlaubt aber Bund, Ländern und Kommunen die gewünschte Registerkonsolidierung.

D. Vorstellung und Bewertung der Ansätze auf Basis einer neuartigen bereichsspezifischen Personenkennziffer

I. Ausgangspunkt: Kern des Regierungsentwurfs-Modells aus technischer Sicht

Abb. 8 | Modell Regierungsentwurf (vereinfacht)

Ausgangspunkt der folgenden Überlegungen hin zu einer datenschutzfreundlicheren Vernetzung staatlicher Register ist das in Teil B bereits erläuterte Modell des RegMoG-E (vgl. **Abbildung 8**). Bereichsübergreifende Datenabfragen laufen grundsätzlich über einen Intermediär – entweder die beim Bundesverwaltungsamt eingerichtete Registermodernisierungsbehörde als Intermediär zum Bundeszentralamt für Steuern (vgl. **Abbildung 9**) oder eine Vermittlungsstelle.

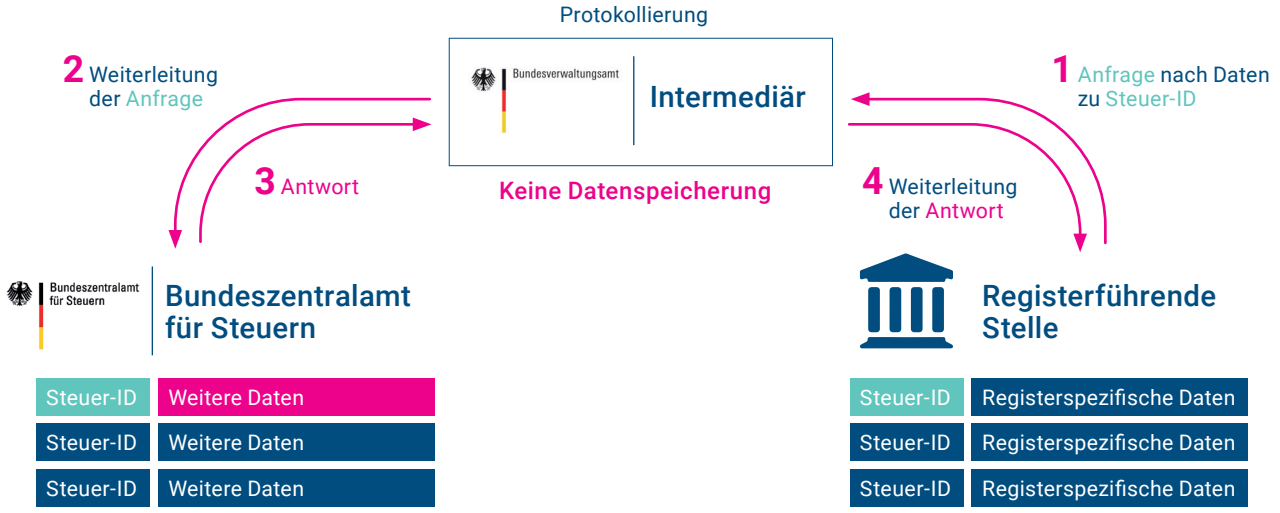
Für den Fall der Übermittlung über eine Vermittlungsstelle ist im Regierungsentwurf das sogenannte 4-Corner-Modell mit „doppeltem Umschlag" vorgesehen. Das bedeutet, dass die eigentlichen Inhalte einer Anfrage so verschlüsselt sind, dass der weiterleitende Intermediär sie nicht zur Kenntnis nehmen kann, sondern lediglich die zur Erfüllung seiner Aufgabe benötigten Metadaten erhält. Dies ist zunächst positiv zu bewerten. Grundsätzlich ist es damit möglich, einen Intermediär so zu betreiben, dass er den Betroffenen nicht identifizieren kann und insbesondere dessen Steuer-ID nicht erhält.

Für die Registermodernisierungsbehörde als Intermediär wird das 4-Corner-Modell im Regierungsentwurf aber gerade nicht gesetzlich normiert.[145] Es ist auch nicht mit der dort verankerten Umsetzung der Prüf- und Protokollierungspflichten vereinbar: Nach § 9 Abs. 1 S. 2 IDNrG-E werden „Datenübermittlungen zwischen der Registermodernisierungsbehörde und dem Bundeszentralamt für Steuern sowie Datenabrufe bei der Registermodernisierungsbehörde […] bei der Registermodernisierungsbehörde protokolliert". Die nach § 10 OZG-E vorgesehene Anzeige im Datencockpit erfordert eine Zuordnung der Protokolldaten zur jeweils betroffenen Person, so dass der potentielle Vorteil, bei der Registermodernisierungsbehörde nicht direkt mit der Steuer-ID umgehen zu müssen, nicht realisiert werden kann. Bezüglich der Vermittlungsstellen wäre dieser Vorteil hingegen noch realisierbar, da § 9 Abs. 1 IDNrG-E hier lediglich die Protokollierung „durch die jeweiligen Stellen" vorschreibt. Eine explizite Klarstellung, dass die Steuer-ID den Vermittlungsstellen nicht zugänglich sein darf, gibt es allerdings nicht. § 7 Abs. 2 S. 4 IDNrG-E fordert lediglich, dass diese ihre „Aufgabe ohne Kenntnis der Nachrichteninhalte erbringen können" müssen. Da die Vermittlungsstellen aber die Übermittlungsberechtigung abstrakt „kontrollieren und protokollieren" (§ 7 Abs. 2 S. 5 IDNrG-E), bleibt unklar, ob die Steuer-ID als Teil des Nachrichteninhalts angesehen wird oder aber Teil der zu protokollierenden Metadaten ist.

[145] Vgl. BfDI 2020, S. 7f. Auch für bereichsinterne Übermittlungen ist das 4-Corner-Modell nicht vorgesehen.

Fest steht allerdings, dass für eine Registermodernisierung nach diesem Konzept eine Verwendung der Steuer-ID als aPK nicht notwendig ist. Indem sie die Zusammenführung von Datensätzen eines Betroffenen unter Umgehung der Intermediäre vereinfacht, führt sie vielmehr zu einem zusätzlichen Risiko[146] und stellt die Rolle der Intermediäre sowie mit ihr die Sicherheitsfunktion des 4-Corner-Modells (s.u.) in Frage. Zur Erreichung der benötigten Funktionalität genügt es, wenn im Zusammenspiel mit dem Intermediär die angefragte Behörde (etwa das Bundeszentralamt für Steuern) die Anfrage zuverlässig einem gespeicherten Datensatz zuordnen und die angeforderten Daten übermitteln kann. Hierfür wird aus technischer Sicht keine gemeinsame ID (aPK) benötigt.[147]

Abb. 9 | Ablauf eines Datenabrufs nach Regierungsentwurf



Für die Weiterentwicklung des Modells ist eine Erkenntnis wichtig: Intermediäre, deren Einführung ohnehin vorgesehen ist, können außer der reinen Weiterleitung von Nachrichten auch zusätzliche Aufgaben erhalten. Statt der Verwendung der Steuer-ID oder eines sonstigen allgemeinen Personenkennzeichens (aPK) ist die Verwendung bereichsspezifischer Personenkennzeichen (bPK) so bereits mit einer kleinen technischen Modifikation des Modells aus dem Regierungsentwurf möglich. Indem die anfallende Aufgabe der Verwaltung von bPK den Intermediären zugeteilt wird, kann ein Zusatzaufwand bei den zahlreichen registerführenden Stellen ganz oder größtenteils vermieden werden.

Als Argument gegen die Einführung von bPK mag angeführt werden, es sei für den Einzelnen nicht leistbar, sich zahlreiche bPK zu merken. Dieses Argument trägt aber aus folgenden Gründen nicht:

→ Auch die Steuer-ID merken sich vermutlich die wenigsten Bürger. Insofern sind mehrere bPK, die die Betroffenen sich ebenfalls nicht merken, keine deutliche Verschlechterung. Die Situation ist vergleichbar mit dem Umgang eines Bürgers mit mehreren Kontonummern, Versicherungsnummern etc.

→ Im Rahmen des E-Government kann Software — oder besser noch, zumindest in einer langfristigen Betrachtung, der Personalausweis — die Aufgabe der Verwaltung mehrerer bPK des Betroffenen, auch direkt im Zusammenhang mit der ohnehin benötigten Authentifizierung, übernehmen.

→ Das ohnehin einzurichtende Datencockpit kann dem Betroffenen nach erfolgter Authentifizierung Auskunft über seine bPK in verschiedenen Bereichen geben. Eine entsprechend gesicherte Abfragemöglichkeit sollte zumindest geprüft werden.

→ Als Authentifizierungsmerkmal, etwa am Telefon, ist die Steuer-ID ohnehin kaum geeignet — dafür ist sie schon jetzt und erst recht bei einer zukünftigen Verwendung als aPK zu vielen Dritten bekannt. Daher bringt es den Betroffenen auch wenig Mehrwert, sich die ID zu merken. bPK könnten in vielen Fällen, zumindest in Ermangelung besserer Alternativen, als ein Authentifizierungsmerkmal unter mehreren durchaus für die telefonische Verwendung geeignet sein.

→ Auch heute schon können Behörden Bürger ohne Vorlage einer Kennziffer identifizieren — im schlimmsten Fall bringen die bPK hier keine Verbesserung.

[146] Vgl. bereits *Sorge/Leicht*, ZRP 2020, S. 242 (243).
[147] Vgl. *Sorge/Leicht*, ZRP 2020, S. 243.

ERGÄNZENDE INFORMATIONEN

Dass die Einführung von bPK auch für Deutschland sinnvoll sein kann, ist durch die Einführung von bPK in Form der „Restricted Identification" des deutschen Personalausweises sowie des elektronischen Aufenthaltstitels in anderem Kontext bereits anerkannt. Dort werden ausweis- und anbieterspezifische Kennziffern erzeugt[148]. Ein direkter Einsatz der so erzeugten Kennziffern für die Registermodernisierung scheidet in der aktuellen Umsetzung zwar deshalb aus, weil die Kennziffern an den konkreten Ausweis und nicht an die Person gebunden sind, sich bei der Ausstellung eines neuen Ausweises also ändern. Das hindert aber weder an einer Einbindung des Ausweises in eine nationale Identitätsmanagement-Strategie noch daran, das Konzept von bPK fortzuentwickeln.

Wir stellen daher in den folgenden Abschnitten technische Modelle für die Umsetzung der Registermodernisierung mit bPK vor.

II. Vorschlag: Einführung neuer bereichspezifischer Personenkennzeichen

Die konkrete Umsetzung von bPK für die Registermodernisierung ist in verschiedenen Varianten möglich.
Abbildung 10 fasst die wesentlichen Optionen zusammen.

Abb. 10 | Morphologischer Kasten zu einem bereichspezifischen Personenkennzeichen

PK / ID-NR	AUSPRÄGUNGSFORMEN				
Einzigartigkeit	einzigartig			mehrfach vergeben	
Sichtbarkeit	nicht-sprechend			sprechend	
Ziffern oder Zeichen und Umfang des Zeichensatzes	numerische Ziffernreihenfolge (0-9)			alphanumerische Zeichenreihenfolge (0-9, A-Z, a-z)	
Prüfziffer	mit Prüfziffer			ohne Prüfziffer	
Typus von Personenkennzeichen	allgemeine Verwendung (aPK: wesentliche Bereiche)		bereichsübergreifende Verwendung (2wPK: 2 oder wenige Bereiche)		bereichsspezifische Verwendung (bPK: 1 Bereich)
Vorgehen bei der Vergabe	zentrale Vergabe			dezentrale Vergabe	
Zu erfassende Personengruppe	Deutsche Bürger	Ausländer	Steuerzahler	Natürliche Personen	Juristische Personen
Basisdatensatz	mit Basisdatensatz			ohne Basisdatensatz	

Wir setzen mit unserem Vorschlag auf ein einzigartiges, nicht-sprechendes Personenkennzeichen. Dieses setzt sich aus mindestens 9 alphanumerischen Zeichen einschließlich einer Prüfziffer zusammen. Die Personenkennzeichen werden zentral vergeben und sollten alle deutschen Staatsangehörigen, alle Unionsbürger und alle Ausländer in Deutschland abdecken. Erfasst werden so alle natürlichen Personen. Die dazugehörigen Stammdaten sollen als Basisdaten gespeichert werden, etwa beim Bundeszentralamt für Steuern.

Mögliche technische Umsetzungen betrachten wir in den folgenden Abschnitten.

Bereits hier sei darauf hingewiesen, dass in keiner Variante die Gefahr einer bereichsübergreifenden Profilbildung völlig ausgeschlossen werden kann: Sobald für irgendeinen (legitimen) Zweck, etwa die Registerkonsolidierung, bPK einander zugeordnet werden können, ist es grundsätzlich möglich, eine solche Zuordnung auch für andere Zwecke zu nutzen.

[148] Vgl. BSI TR 03110 Part 2, Version 2.21, S. 31 f.

III. Stammzahl-Modell

Abb. 11 | Bereichsspezifische Personenkennziffer nach dem Stammzahl-Modell

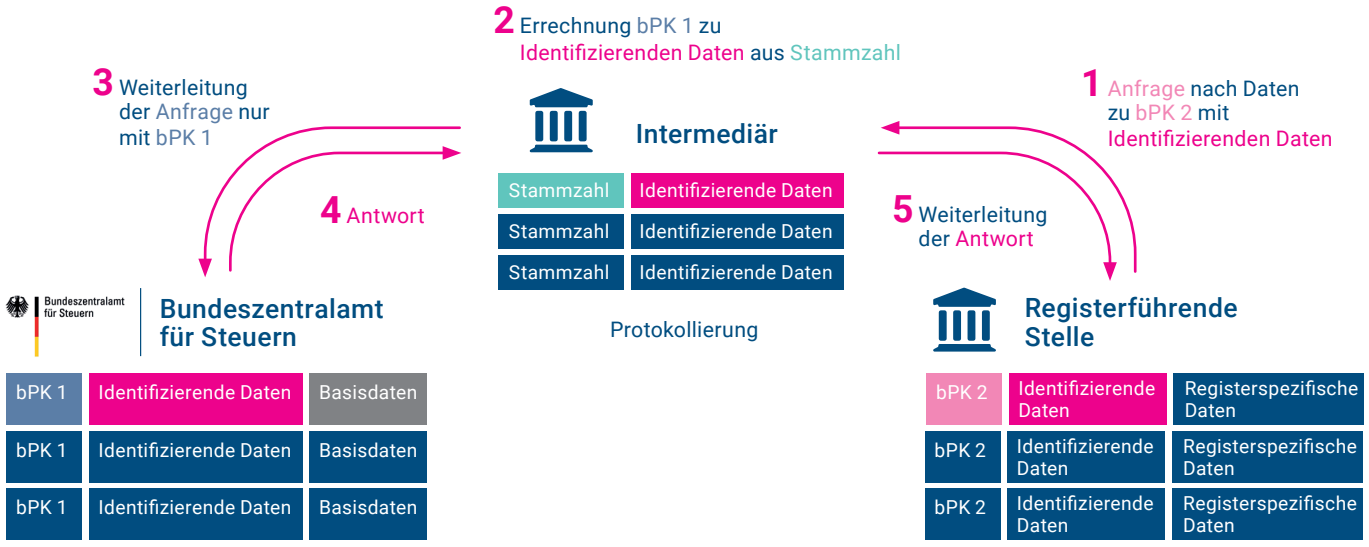
Abbildung 11 zeigt die Struktur einer Variante zur Umsetzung von bPK für die Registermodernisierung, die auf dem österreichischen Modell bereichsspezifischer Personenkennzeichen beruht.[149] Die österreichische Registerstruktur unterscheidet sich von der deutschen, so dass eine vollständige Übernahme des österreichischen Modells nicht möglich ist; der technische Kern ist aber übertragbar.

Hier wird jeder Person eine *Stammzahl* zugeordnet, die geheim gehalten wird und nicht vorhersehbar bzw. erratbar sein darf. Beispielsweise könnte jedem Inhaber einer Steuernummer eine ausreichend lange Zufallszahl als Stammzahl zugeordnet werden.

Die bPK wird aus der Stammzahl abgeleitet, indem eine kryptographische Hashfunktion auf die Stammzahl und die Bezeichnung des Bereichs (etwa „Steuer“) angewendet wird. Kryptographische Hashfunktionen garantieren – neben anderen Eigenschaften – dass aus der bPK nicht auf die Stammzahl zurückgeschlossen werden kann.[150] Auch lassen sich ohne Kenntnis der Stammzahl die bPK der gleichen Person für verschiedene Bereiche einander nicht zuordnen. Die Ausgabe einer kryptographischen Hashfunktion wird gelegentlich auch als „Fingerabdruck“ bezeichnet.[151] Kryptographische Hashfunktionen sind in der IT-Sicherheit schon lange etabliert; unter anderem werden sie im Rahmen der Erzeugung digitaler Signaturen eingesetzt und sind eine wesentliche technische Grundlage von Blockchains.

Auch, wenn die Stammzahl nicht aus einer bPK errechnet werden kann, wäre es denkbar, dass ein Angreifer systematisch Stammzahlen durchprobiert, zugehörige bPK mit Hilfe der Hashfunktion ableitet und mit tatsächlich vergebenen bPK vergleicht. Dem begegnet man mit einer ausreichenden Länge der Stammzahlen, die sich an der Länge der Schlüssel symmetrischer Verschlüsselungsverfahren orientieren kann (128 bis 256 bit).[152]

Abb. 12 | Ablauf eines Datenabrufs im Stammzahl-Modell



Will nun eine Behörde Daten aus einem anderen Bereich abfragen, schickt sie – in gleicher Weise wie im Regierungsentwurf vorgesehen – eine Anfrage an den Intermediär, dem die Stammzahl vorliegt (vgl. **Abbildung 12**).

Hier ergibt sich zunächst eine Schwierigkeit bei der Zuordnung der Anfrage zu einer Stammzahl durch den Intermediär. Aus der bPK kann auch der Intermediär die Stammzahl nicht berechnen. Ohne weitere Informationen hat er keinen Anhaltspunkt, welche der bei ihm gespeicherten Stammzahlen zu der bPK aus der Anfrage passt. Folglich benötigt er zumindest einen Minimaldatensatz zur Identifikation der Person, zu der eine Stammzahl gehört – etwa Nachname, Geburtstag und Geburtsort.[153] Dieser Datensatz ist folglich beim Intermediär zu speichern (oder muss zumindest für ihn abrufbar sein). Auch in der Anfrage muss dieser Datensatz so übermittelt werden, dass der Intermediär darauf zugreifen kann – bei Verwendung des Konzepts „doppelter Umschlag" muss der Datensatz also Teil der Metadaten einer Anfrage sein und nicht nur Teil der Inhaltsdaten im „inneren Umschlag", den der Intermediär nur verschlüsselt weiterleitet. Der Datensatz muss keine eindeutige Identifikation zulassen; kommen mehrere Personen in Frage, kann der Intermediär jeweils die bPK der entsprechenden Person ableiten, bis die bPK aus der Anfrage gefunden wird.

Der Intermediär berechnet nun (in Schritt 2) die bPK des anderen Bereichs und leitet die Anfrage gemeinsam mit der errechneten bPK (im Bild: bPK1) weiter. Auch bei der Weiterleitung der Antwort wird die dort enthaltene bPK wieder ersetzt.

Der Ansatz vermeidet damit die Verwendung einer einzelnen aPK, die zahlreichen Behörden und Unternehmen bekannt ist. Die sich ergebende Registerarchitektur ist sehr ähnlich zu der aus dem Regierungsentwurf. Es entsteht geringer Mehraufwand bei den Intermediären, wohingegen in den eingebundenen Registern lediglich eine bPK statt der Steuer-ID verwendet werden muss. Die Verschlüsselung der Kommunikationsinhalte kann in gleicher Weise wie im Regierungsentwurf, insbesondere auch nach dem Konzept des „doppelten Umschlags", umgesetzt werden. Voraussetzung ist lediglich die Übermittlung des jeweiligen bPK (sowie der o.g. identifizierenden Minimaldaten) in den Metadaten statt als Teil der verschlüsselten Inhaltsdaten, um deren Zuordnung durch den Intermediär zu ermöglichen.

Da der Intermediär die bPK aller Bereiche ableiten kann, ist neben einer zentralen Speicherung von Basisdaten bei einer Stelle (wie dem Bundeszentralamt für Steuern) auch eine verteilte Variante denkbar, bei der auf Daten unterschiedlicher Bereiche zurückgegriffen werden muss.

Eine Stärke des Ansatzes besteht darin, dass auch bei der Einführung neuer Behörden bzw. Bereiche die Ableitung von bPK nur anhand von Stammzahl und Bereichsbezeichner möglich ist. Dies ermöglicht perspektivisch eine einfache Integration in Systeme wie den elektronischen Personalausweis. Dieser bringt bereits die technische Basis für die sichere Speicherung der Stammzahl mit und könnte dezentral bPK erzeugen – selbst wenn die entsprechende Behörde bzw. der entsprechende Bereich zum Ausstellungszeitpunkt des Ausweises noch nicht existierte.

Unter Umständen könnte der Ansatz damit eine vertretbare Lösung darstellen, die im Vergleich mit dem gegenwärtigen Regierungsentwurf eine Verbesserung des Datenschutz- und Sicherheitsniveaus erreichen kann.

Er leidet aber unter mehreren Schwächen:

→ Bestehende IDs können nicht einfach integriert werden, sondern müssen durch neuartige bPK ersetzt oder ergänzt werden.

→ Um Kollisionsfreiheit (Ausschluss mehrfacher Verwendung der gleichen bPK) zu garantieren, müssen die bPK lang sein. Aktuelle Hashfunktionen haben oft eine Ausgabe mit einer Länge von 256 bit, was zwar für die Verwendung in IT-Systemen völlig unproblematisch ist. Sollen jedoch in der Praxis Menschen mit den bPK umgehen (z.B. Eintrag in Papierformulare oder Übermittlung per Telefon), ist eine Kürzung auf 80 bis 100 bit vermutlich möglich, ohne das Risiko zufälliger Kollisionen einzugehen. Dies entspricht aber immer noch einer mindestens 16stelligen alphanumerischen (also aus Buchstaben und Ziffern bestehende) Zeichenfolge.

→ Verwendet man als Intermediär lediglich eine zentrale Behörde, so hat dieser die Fähigkeit, alle bPK aller eingetragenen Personen einander zuzuordnen.[154] Das erhöht zwar die Flexibilität der Lösung. Jedoch bedeutet die grundsätzlich beliebige Zuordnungsmöglichkeit auch die Gefahr einer Profilbildung, wenn keine entgegenwirkenden technischen und organisatorischen Maßnahmen getroffen und dauerhaft aufrechterhalten werden. Gleichzeitig ist der Intermediär ein „Single Point of Attack". Im Fall eines erfolgreichen

[149] Vgl. Zum österreichischen Modell, insb. zur Erzeugung und zum Schutz von Stammzahl und bPK §§ 6 ff. des österreichischen E-GovG (Öst. Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen, E-Government-Gesetz – E-GovG).

[150] Vgl. *Stallings* 2017, Cryptography and Network Security (7th edition), S. 349.

[151] Vgl. *Katz/Lindell* 2014, Introduction to Modern Cryptography (2nd edition), S. 182.

[152] Bei 128 bit gibt es 2^{128} Möglichkeiten (340282366920938463463374607431768211456 oder ca. $3{,}4*10^{38}$ in Dezimalschreibweise), bei 256 bit sind es 2^{256} oder $1{,}16*10^{77}$ Möglichkeiten – also eine 78stellige Zahl. Schon bei 128 bit ist systematisches Durchprobieren nicht realistisch möglich.

[153] Alternativ kann bei einem Intermediär, der die Rolle der Vermittlungsstelle aus dem Regierungs-entwurf übernimmt, auch eine Tabelle mit Zuordnungen der bPK nur aus den vom Intermediär betreuten Bereiche gespeichert werden. In diese Umsetzung entstünde eine Mischform aus dem Stammzahl-Modell und dem unten vorgeschlagenen Neu-ID-Ansatz.

[154] Dies gilt, obwohl die bPK im Normalbetrieb nicht gespeichert werden. Gehen wir von je 100 bPK aus, die aus bereits vorliegenden Stammzahlen von ca. 100 Millionen Personen abgeleitet werden. Insgesamt wären dies 10 Milliarden bPK. Aktuelle Grafikkarten schaffen bis ca. 1 Milliarde Hashberechnungen pro Sekunde, könnten diese Berechnung also in 10 Sekunden durchführen; spezielle Hardware schafft die etwa für Bitcoin Mining notwendigen Hashberechnungen mit einer Rate von über 10 Billionen Berechnungen pro Sekunde, wäre also theoretisch in einer Millisekunde fertig. Durch Begrenzungen praktischer Rechnerarchitekturen mögen sich die Vorgänge etwas verlängern; sie stellen aber jedenfalls kein Hindernis für einen motivierten Angreifer dar. Anschließend lassen sich die bPK ohne nennenswerten Aufwand einander zuordnen. Zwar gibt es Techniken, die den Vorgang der Hashberechnung verlangsamen. Eine solche Verlangsamung wirkt sich aber im gleichen Maß auf die Ableitung der bPK im Normalbetrieb aus. Wenn die Ableitung von bPK schnell genug sein muss, um auch bei Lastspitzen im Normalbetrieb zu funktionieren, kann sie nicht gleichzeitig langsam genug sein, um Missbrauch durch Erzeugung von Tabellen mit allen bPK aller Personen zu verhindern. Es sind folglich ergänzende Maßnahmen erforderlich.

Angriffs oder Missbrauchs fällt die Lösung schlimmstenfalls auf den Stand des Regierungsentwurfs zurück.

→ Verteilt man die Rolle des Intermediärs auf mehrere Stellen – wie im Ansatz durch die Einführung von Vermittlungsstellen bereits in § 7 Abs. 2 IDNrG-E vorgesehen –, so gibt es zwei Möglichkeiten: Entweder werden bei jeder dieser Stellen die Stammzahlen aller Personen gespeichert, für die die Vermittlungsstelle zuständig ist. Diese Möglichkeit bedeutet somit aber auch mehr Angriffspunkte und Missbrauchsmöglichkeiten bzw. aus anderer Sicht einen höheren Aufwand für die Absicherung der Stammzahlen. Oder es wird eine Hierarchie von Stammzahlen und bPK erzeugt: Aus der zentralen Stammzahl werden bPK wie oben beschrieben erzeugt und an Vermittlungsstellen gegeben, die daraus wiederum nach dem gleichen Prozess Unter-bPK für die ihnen zugeordneten Bereiche erzeugen. Das ist technisch machbar, gerade bei sich überschneidenden Zuständigkeiten von Vermittlungsstellen erhöht sich die Komplexität des Systems damit aber erheblich.

→ Da alle bPK bei diesem Ansatz aus einer Stammzahl abgeleitet werden, ist die Neuvergabe einer bPK (etwa im Fall eines „Identitätsdiebstahls") mit der Neuvergabe der Stammzahl und damit aller anderen bPK verbunden.

Insgesamt kann festgehalten werden, dass dieses Modell gegenüber dem des Regierungsentwurfs bereits deutlich datenschutzfreundlicher und auch mit nur geringem Mehraufwand umsetzbar ist. Die Nachteile des Ansatzes fallen aber durchaus ins Gewicht, so dass keine uneingeschränkte Empfehlung dafür ausgesprochen werden kann. Eine Übersicht der wesentlichen Stärken und Schwächen in Form einer SWOT-Analyse ist in Abbildung 13 dargestellt. Im Folgenden entwickeln wir den Alternativansatz NEU-ID, der die benannten Schwächen weitgehend vermeidet.

Abb. 13 | SWOT-Analyse zum Identitätsnummernsystem Stammzahl-Modell

STÄRKEN

- → Bereits deutlich datenschutzfreundlicher im Vergleich zum Regierungsentwurf
- → Weitestgehendes Beibehalten der aktuellen Registerstruktur möglich
- → Verzicht auf Einführung einer aPK
- → Datenaustausch zwischen Behörden ohne Kenntnis der jeweils anderen bPK möglich
- → bPK für neu eingeführte Bereiche mit Kenntnis der Stammzahl jederzeit einfach errechenbar (auch z.B. bei Umsetzung im Personalausweis)

SCHWÄCHEN

- → Notwendigkeit, bei den Intermediären identifizierende Daten zu speichern
- → Intermediäre werden zu einem attraktiveren Ziel für Angreifer
- → Notwendigkeit, bPK neu zu generieren
- → Länge der bPK erschwert Handhabung etwa am Telefon
- → Erhöhter Aufwand bei verteilter Realisierung

CHANCEN

- → Reichweitenbegrenzung von Profilbildungen durch bPK
- → Einbindung des Personalausweises perspektivisch möglich
- → Reduktion der Datenspeicherung in einzelnen Registern durch einfache und datenschutzkonforme Abrufmöglichkeiten

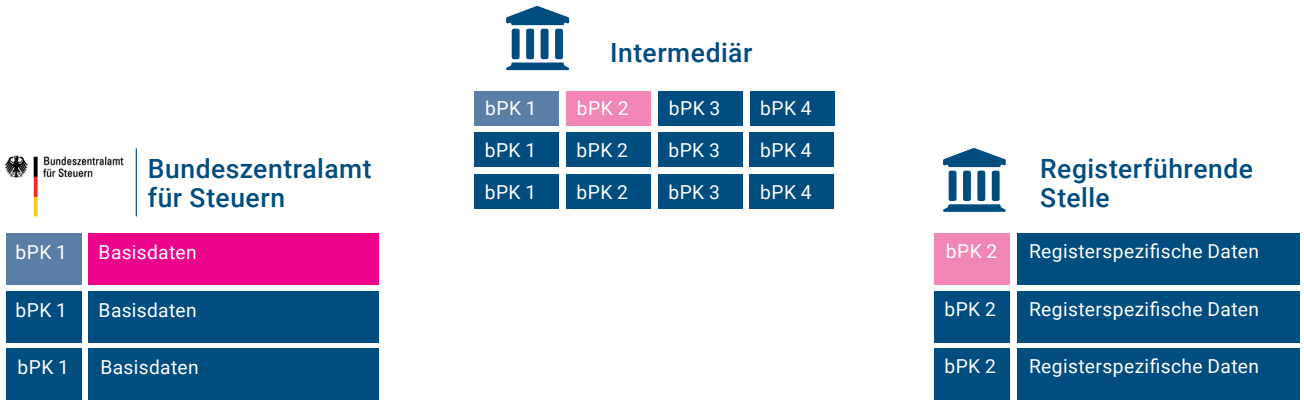
RISIKEN

- → Weiterhin bestehende, wenn auch gemilderte Gefahr bereichsübergreifender Datenzusammenführung zur Profilbildung
- → Möglichkeit der Erstellung von Transaktionsprofilen
- → Möglichkeit von Datenpannen bei den Intermediären

IV. Neuartige bereichsspezifische Personenkennzeichen (NEU-ID)

Statt des Minimaldatensatzes speichert der Intermediär die bPK verschiedener Bereiche bei diesem Ansatz selbst. Somit liegt beim Intermediär – nur – eine Tabelle vor, die für jede Person eine Liste von bPK enthält, aber keine weiteren Informationen zur Person (vgl. **Abbildung 14**). Die Festlegung einer Stammzahl ist bei dieser Variante nicht erforderlich. Bei den Intermediären, die die Rolle der Vermittlungsstellen aus dem Regierungsentwurf übernehmen, sind diejenigen Teile der Tabelle gespeichert, die für die konkrete Aufgabenerfüllung benötigt werden: Soll zwischen zwei Bereichen vermittelt werden, werden auch nur die bPK dieser beiden Bereiche gespeichert.

Abb. 14 | Grundkonzept NEU-ID

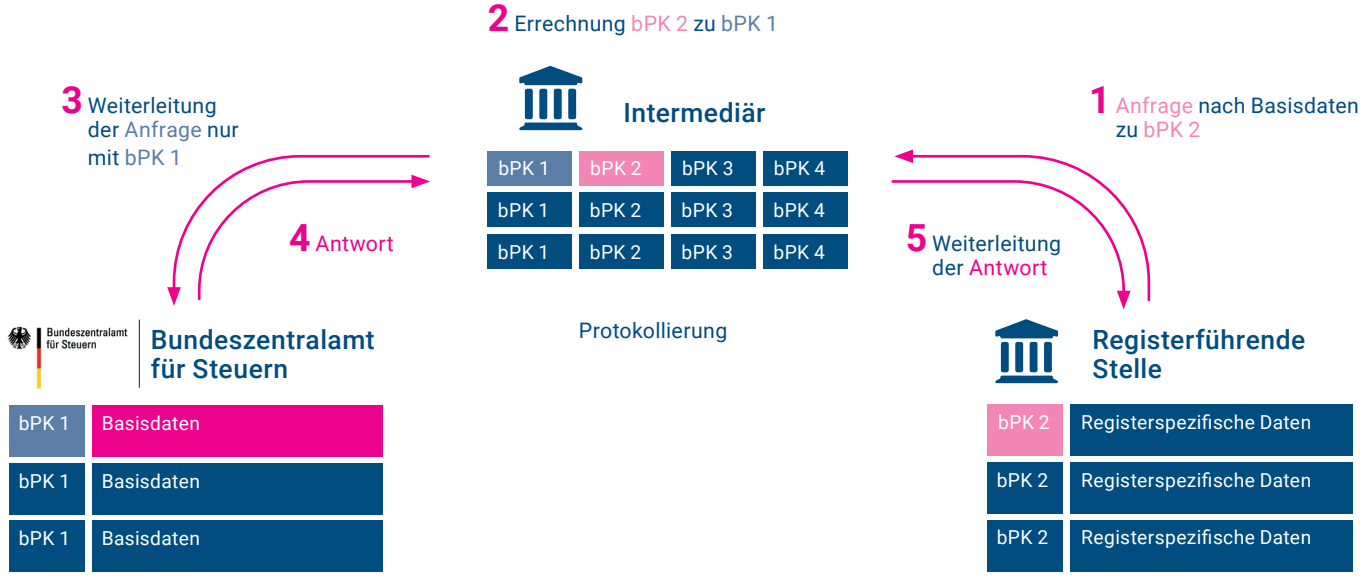


bPK müssen nicht mehr die Ergebnisse von Hash-Berechnungen sein. Die Speicherung der bPK in einer Tabelle erlaubt einerseits die Weiterverwendung bereits bestehender bPK wie der Steuer-ID. Andererseits können neue bPK erzeugt werden. Diese können deutlich kürzer sein als im oben dargestellten Stammzahl-Modell – wo die Länge der bPK zufällige „Kollisionen", also doppelt erzeugte bPK, vermeiden soll. Die Gefahr, dass zufällig zwei identische bPK erzeugt werden, besteht nämlich deshalb nicht, weil neu erzeugte bPK einfach in der bestehenden Tabelle mit den bereits bestehenden abgeglichen werden können. Da keine Anforderung besteht, dass eine bPK ein Hashwert einer Stammzahl sein muss, kann im Fall einer solchen Kollision die bPK schlicht so oft zufällig neu erzeugt werden, bis keine Kollision mehr auftritt.

Die Erzeugung kann in den einzelnen Bereichen oder – um einfacher die Kollisionsfreiheit zu garantieren – beim (zentralen) Intermediär vorgenommen werden. Um die Handhabung außerhalb von IT-Systemen fehlertolerant zu gestalten, sollte eine Prüfziffer[155] verwendet werden.

Abbildung 15 zeigt beispielhaft den Ablauf bei einem Datenabruf vom Bundeszentralamt für Steuern. Ganz wie im Stammzahl-Modell übernimmt der Intermediär die Zuordnung von bPKs und sorgt dafür, dass die bPK eines Bereichs nicht an einen anderen Bereich weitergeleitet wird. Hier wird auch nochmals deutlich, dass der Intermediär für die Zuordnung keinerlei andere Daten braucht als die bPK selbst. Ist der Intermediär, etwa als Vermittlungsstelle, nur für wenige Bereiche zuständig, benötigt er auch nur die bPK dieser Bereiche.

Abb. 15 | Ablauf eines Datenabrufs im NEU-ID-Modell



[155] Eine Prüfziffer (vgl. Abschnitt A.III) wird der eigentlichen ID angehängt oder vorangestellt. Sie wird nach einer öffentlich bekannten Rechenvorschrift berechnet. Wird die ID nebst Prüfziffer eingegeben, so kann die neu errechnete Prüfziffer mit der eingegebenen verglichen und ein Eingabefehler mit hoher Wahrscheinlichkeit erkannt werden.

Eine Risikoerhöhung im Vergleich zum oben beschriebenen Stammzahl-Modell scheint sich dadurch zu ergeben, dass die Zuordnung unterschiedlicher bPK den Intermediären jederzeit möglich ist. Tatsächlich ist dies beim Stammzahl-Modell aber auch so, denn dort liegen die zur Berechnung der bPK erforderlichen Informationen ebenfalls vor – wenn auch nicht in sofort verfügbarer und nutzbarer Form, sondern nur als Stammzahl.[156] Die wesentlichen, oben aufgeführten Vorteile blieben bei der neuen Variante erhalten. Da der Intermediär die benötigten bPK kennt, reicht es, wenn Anfragen seitens einer registerführenden Stelle deren bPK als Teil der Metadaten beinhalten. Weitere identifizierende Daten, wie beim Stammzahl-Modell vorgesehen, müssen weder an den Intermediär übermittelt noch dort gespeichert werden. Ist der anfragenden Stelle keine bPK bekannt, wird diese wie bereits im RegMoG-E nach dem 4-Corners-Modell vorgesehen verschlüsselt an die Stelle (im Beispiel: Bundeszentralamt für Steuern) weitergeleitet, die die Basisdaten speichert. Die Antwort enthält eine bPK, die dann wiederum in die bPK des anfragenden Bereichs übersetzt wird. Risiken, die sich bereits grundsätzlich aus dem Vorhandensein einer Zuordnung von bPK ergeben, bleiben bestehen.

Die technische Umsetzung des Ansatzes ist völlig unproblematisch. Rechnet man – auch zukünftige Generationen berücksichtigend – mit einer Milliarde Personen, die jeweils 100 bPK[157] benötigen, müssen 100 Milliarden unterschiedliche bPK möglich sein. Dies gilt jedenfalls, wenn die gleiche bPK nicht in mehreren Bereichen (auch für unterschiedliche Personen) verwendet werden soll. Ein solches bPK kann in weniger als 5 Byte[158] (ggf. zzgl. einer Prüfziffer, die aber beim Intermediär nicht gespeichert werden müsste) repräsentiert werden, so dass alle bPK der derzeit in Deutschland lebenden Personen in unter 50 Gigabyte Speicher unterzubringen wären.[159] Auf dem heutigen Stand der Technik sind solche Datenmengen problemlos handhabbar; schon gängige Smartphones haben eine höhere Speicherkapazität. Die angenommenen Werte sind dabei eher hoch gegriffen – vermutlich genügen deutlich weniger als 100 bPK pro Person. Zu den Stärken des Ansatzes gehört, dass eine solche kurze bPK praktisch für die menschliche Verwendung ist und beispielsweise auch telefonisch durchgegeben werden kann – etwa als 9-stellige alphanumerische Zeichenfolge (also Buchstaben und Ziffern)[160] oder in 4 Codewörtern (z.B. „Kellner Straße Maus Montag").

Auch bei dieser Variante besteht die Möglichkeit der Profilbildung unter Mitwirkung des Intermediärs. Dieser hat zwar wenige Informationen über einzelne Personen und kennt insbesondere nicht ihre Namen. Die jeweiligen bPK sind aber dennoch als personenbezogene Daten einzuordnen (vgl. zum Begriff Abschnitt B.II). Im dargestellten Grundmodell genügt es insbesondere beim zentralen Intermediär, wenn dieser Kenntnis über eine einzelne bPK erlangt, um einer Person all ihren anderen bPK zuordnen zu können. Missbrauch durch Innentäter oder erfolgreiche Angriffe auf den Intermediär lassen die Variante, ebenso wie das oben dargestellte Stammzahl-Modell, auf das Datenschutz- und Sicherheitsniveau des Regierungsentwurfs zurückfallen.

Die wesentlichen Stärken und Schwächen des NEU-ID-Ansatzes sind in **Abbildung 16** zusammengefasst.

Abb. 16 | SWOT-Analyse zum Identitätsnummernsystem NEU-ID

STÄRKEN

- •Wesentlich datenschutzfreundlichere und zugleich funktionale Implementierungsvariante
- Weitestgehendes Beibehalten der aktuellen Registerstruktur möglich
- Verzicht auf Einführung einer aPK
- Datenaustausch zwischen Behörden ohne Kenntnis der jeweils anderen bPK möglich
- Kurze bPK erleichtern Nutzung etwa am Telefon
- Speicherung ausschließlich von bPK bei den Intermediären

SCHWÄCHEN

- Weitgehend zentralisierte Verwaltung und Vergabe von bPK notwendig
- Intermediäre werden zu einem attraktiven Ziel für Angreifer (vgl. Stammzahl-Modell)

CHANCEN

- Reichweitenbegrenzung von Profilbildungen durch bPK
- Eignung des Ansatzes für die weitere Verteilung von Identitätsmanagement-Aufgaben mit föderalem Ansatz
- Einbindung des Personalausweises perspektivisch möglich
- Reduktion der Datenspeicherung in einzelnen Registern durch einfache und datenschutzkonforme Abrufmöglichkeiten

RISIKEN

- Weiterhin bestehende, wenn auch gemilderte Gefahr bereichsübergreifender Datenzusammenführung zur Profilbildung
- Möglichkeit der Erstellung von Transaktionsprofilen
- Möglichkeit von Datenpannen bei den Intermediären

V. Optionen für die Verbesserung beider Modelle

Zusätzlich kommen einige Lösungsansätze in Frage, die zusammengenommen weiter dazu beitragen können, die oben dargestellten Risiken zu reduzieren – ob beim NEU-ID-Modell oder beim Stammzahl-Modell. Wir beschreiben diese in den folgenden Abschnitten.

1. Institutionelle Unabhängigkeit des Intermediärs

Die Einrichtung des zentralen Intermediärs beim Bundesverwaltungsamt – einer Behörde im Geschäftsbereich des BMI – ist aus fachlicher Sicht nachvollziehbar. Das Vertrauen in die auch langfristig sichergestellte, ausschließlich zweckgebundene Verwendung der Zuordnungsmöglichkeiten ließe sich aber durch die Einrichtung bei einer unabhängigen, nicht weisungsgebundenen Stelle erheblich erhöhen, weshalb wir diese Variante als klar vorzugswürdig ansehen. Denkbar ist dies etwa unter der administrativen Verantwortung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit oder der Datenschutzbeauftragten der Bundesländer (vgl. nächster Punkt). Für zusätzliche Vermittlungsstellen, wie im Regierungsentwurf angelegt, gilt im Prinzip das Gleiche; allerdings ist hier eine Risikoreduktion je nach konkreter Funktion zumindest beim NEU-ID-Modell auch denkbar, indem dort lediglich die bPK sehr weniger Bereiche gespeichert werden (s.u.).

Weitere Aufgaben der Registermodernisierungsbehörde neben der Intermediärsrolle werden durch diesen Vorschlag nicht berührt.

2. Föderierter Ansatz

Ein sogenanntes föderiertes Identitätsmanagement, bei dem auf eine zentrale Datenbank mit Identitätsinformationen verzichtet wird, ist bereits gängig.[161] Es setzt lediglich Vertrauen zwischen den Institutionen voraus, die die Identitäten (und ggf. Authentifizierung) der anderen Teilnehmer des föderierten Identitätsmanagement-Systems anerkennen und nutzen. Dies lässt sich, wie schon die Bezeichnung nahelegt, leicht mit der föderalistischen Struktur der Bundesrepublik Deutschland in Einklang bringen. Angesichts der Bedeutung der Verwaltungshoheit der Länder wären zumindest Ansätze eines föderierten Identitätsmanagements auch im Rahmen der Registermodernisierung nach Auffassung der Autoren ohnehin wünschenswert. Verschiedene Umsetzungsvarianten sind denkbar. Die einfachste Lösung wäre wohl, die zentrale Intermediärsrolle[162] zwar beizubehalten, aber statt einer Bundesbehörde je einen zuständigen Intermediär pro Bundesland vorzusehen – was Verwaltungskooperationen mehrerer Länder natürlich nicht ausschließt. Die Identifikation des jeweils zuständigen Intermediärs anhand des Wohnsitzlandes dürfte sich unproblematisch gestalten. Im Einzelfall, wenn das aktuelle Wohnsitzland der anfragenden Stelle nicht bekannt ist, kann sich die Notwendigkeit ergeben, eine Anfrage an alle in Frage kommenden Intermediäre zu senden.

Für die Erzeugung der bPK müssen den Intermediären im NEU-ID-Modell jeweils Nummernbereiche zugeordnet werden. Beim Stammzahl-Modell kann dies entfallen, da die Stammzahlen ohnehin so lang sein müssen, dass zufällige Kollisionen nicht auftreten. In beiden Modellen sind Vorkehrungen für die Übermittlung von Datensätzen bei Umzug und Konsistenzprüfungen zu treffen. Eine Anbindung an das geplante Datencockpit lässt sich leicht ergänzen – in gleicher Weise, wie dies für die Intermediäre (Registermodernisierungsbehörde, Vermittlungsstellen) des Regierungsentwurfs möglich ist. Alle weiteren Abläufe blieben bei diesem Ansatz unverändert. Die höhere Anzahl an Intermediären bedeutet in der Summe vermutlich höhere Kosten, insbesondere angesichts des Aufwands zur Absicherung – allerdings wird gleichzeitig die Problematik des „Single Point of Attack" abgemildert. Die Funktion der Vermittlungsstellen lässt sich in vergleichbarer Weise verteilt realisieren; wenn diesen aber jeweils nur die bPK weniger Bereiche vorliegen, kann im NEU-ID-Modell ggf. auch eine zentralisierte Umsetzung unter Umständen vertretbar sein.

3. Bürger als lokale Intermediäre

Die Intermediärsfunktion muss nicht in allen Fällen überhaupt durch eine Behörde ausgeübt werden. So ließe sich für viele Verfahren als Regelfall die Übernahme der Funktion durch den Betroffenen selbst – technisch umgesetzt entweder in einer App, die digital signierte Informationen von den zuständigen Behörden speichert und verwaltet, ohne allerdings die Daten an den technischen Betreiber des Betriebssystems oder der App weiterzugeben, oder in einer Weiterentwicklung des elektronischen Personalausweises – etablieren. Der Rückgriff auf die Datenbank bei einer Behörde wäre dann nur noch in Fällen notwendig, bei denen der Betroffene nicht mitwirken kann oder will – also z.B. bei Verlust des Ausweises oder bei Vorgängen wie dem Zensus,

[156] Vgl. Fn. 153.

[157] Der Regierungsentwurf (§ 7 Abs. 2 S. 2) geht von mindestens sechs Bereichen aus, bei denen eine bereichsübergreifende Kommunikation unter Einschaltung von Vermittlungsstellen realisiert wird. Die tatsächlich sinnvolle Zahl einzurichtender Bereiche wird vermutlich über sechs, aber deutlich unter den 100 Bereichen der hier vorgenommenen, bewusst großzügigen Abschätzung liegen.

[158] 5 Byte entsprechen 40 bit. Das genügt, um 2^{40} Möglichkeiten zu repräsentieren; dies entspricht etwa 1,1 Billionen oder ca. dem Zehnfachen der nach obiger Rechnung benötigten 100 Milliarden. Für deren Repräsentation würden 37 bit genügen, doch sind ganze Byte in der Ver¬arbeitung ggf. einfacher und lassen eine Reserve für mögliche Erweiterungen. Lässt man zu, dass die gleiche bPK in mehreren Bereichen – dann für jeweils andere Personen – gültig ist, lässt sich die Länge auf 30 bit reduzieren.

[159] Bei der Weiterverwendung bereits bestehender bPK wird sich der Speicherbedarf etwas ändern, nicht aber dessen Größenordnung.

[160] Um 40 bit in 8 Stellen – also 5 bit pro Stelle – zu codieren, muss es pro Stelle 32 Möglichkeiten geben, also 10 Ziffern zzgl. 22 Buchstaben. Die 9. Stelle kann als Prüfziffer dienen. Das gleiche Prinzip lässt sich für Codewörter anwenden. Lässt man 4096 gültige Wörter zu, entspricht dies 12 bit pro Wort. In 4 Codewörtern lässt sich die bPK also einschließlich einer Prüfziffer darstellen.

[161] Etwa im elektronischen Rechtsverkehr nach dem SAFE-Standard („Secure Access to Federated E-Justice/E-Government"), vgl. https://www.it-planungsrat.de/DE/Projekte/Anwendungen/SAFE/sAFE.html

[162] Also die im Regierungsentwurf für die Registermodernisierungsbehörde beim Bundesverwaltungs¬amt vorgesehene Rolle beim Abruf und der Übermittlung von Daten.

die eine Mitwirkung des Einzelnen zu aufwendig erscheinen lassen. Diese Variante dürfte sich kurzfristig nur schwer umsetzen lassen, erscheint mittelfristig aber aus Gründen des Datenschutzes und der Transparenz durchaus erwägenswert. Eine besonders elegante Umsetzung der Variante ist im Stammzahl-Modell möglich, da mit Kenntnis der Stammzahl eine einfache Erzeugung von bPK auch für im Vorhinein nicht festgelegte Bereiche besteht.

4. Einschränkung möglicher Zuordnungen

In der bisherigen Darstellung haben wir die Einschränkung möglicher Zuordnungen zwischen den bPK verschiedener Bereiche nicht problematisiert – also die Frage, ob grundsätzlich bPK aus jedem Bereich in bPK jedes anderen Bereichs überführt werden können sollen. Der Regierungsentwurf geht aber bereits davon aus, dass keine beliebigen Kommunikations-beziehungen zwischen registerführenden Stellen unterschiedlicher Bereiche zugelassen sind. Neben dem Abruf der Basisdaten, die beim Bundeszentralamt für Steuern gespeichert werden, sind nach § 7 Abs. 2 IDNrG-E auch sonstige Datenübermittlungen zwischen öffentlichen Stellen möglich; hier wird aber die abstrakte Übermittlungsberechtigung durch eine Vermittlungsstelle geprüft, die also die Rolle eines Intermediärs einnimmt. Dieses Konzept sollte in dem von uns vorgeschlagenen Modell nicht nur beibehalten werden; vielmehr sollten auch die Zuordnungen von bPK, die für legitime Zwecke nicht benötigt werden, weitestgehend technisch verhindert werden. Will man Basisdaten weiterhin beim Bundeszentralamt für Steuern speichern, wären Anfragemöglichkeiten des dafür verwendeten Intermediärs also auf die Zuordnung eines beliebigen andere bPK auf die beim Bundeszentralamt für Steuern verwendete bPK (vermutlich die Steuer-ID) und umgekehrt beschränkt.

Auch die im Regierungsentwurf vorgesehenen Vermittlungsstellen dürfen keine beliebigen Zuordnungen vornehmen. bPK von Bereichen, aus denen andere Bereiche keine Daten abrufen müssen oder für die die Vermittlungsstelle nicht zuständig ist, dürfen dort nicht dauerhaft gespeichert werden. Im Stammzahl-Modell lässt sich dies nur eingeschränkt umsetzen, etwa wie oben beschrieben durch die Nutzung einer Hierarchie von Stammzahlen und bPK. Das NEU-ID-Modell erlaubt hier eine einfache, recht flexible Umsetzung. Auch dort kann es aber vorkommen, dass einer Vermittlungsstelle mehr Zuordnungen möglich sind, als tatsächlich vorgenommen werden dürfen. Entsprechende Einschränkungen sind zumindest durch Zugriffsregeln durchzusetzen. Wie im Regierungsentwurf vorgesehen,[163] dürfen Anfragen, bei denen abstrakt keine Übermittlungsberechtigung vorliegt, nicht beantwortet werden und sind zu protokollieren. Der Unterschied zum Regierungsentwurf liegt in unserem Ansatz darin, dass dem Anfragenden aus einem anderen Bereich die Ziel-bPK nicht vorliegt und eine Umgehung des Intermediärs somit erschwert wird.

5. Technische Sicherheit

Selbstverständlich ist der Intermediär nach dem Stand der Technik abzusichern. Dies ergibt sich – neben den Erwägungen aus dem nationalen Verfassungsrecht[164] – auch unionsrechtlich aus Art. 87 DSGVO i.V.m. Art. 5 Abs. 1 lit. f) und Art. 24 DSGVO.[165] Dieser sieht vor, dass die Verwendung von nationalen Kennziffern, sowie von anderen Kennziffern von allgemeiner Bedeutung, nur unter Wahrung geeigneter Garantien für die Rechte und Freiheiten der betroffenen Personen zulässig ist. Der Gesetzgeber muss diese Garantien daher u.a. durch geeignete technische und organisatorische Maßnahmen sicherstellen.[166] Aufgrund der hohen Anzahl potentiell Betroffener im Fall einer Verletzung des Schutzes der gespeicherten personenbezogenen Daten ist ein strenger Maßstab an diese Vorkehrungen anzulegen.[167]

Ein geeignetes Mittel, das bei beiden Modellen in die entsprechende Sicherheitsarchitektur integriert werden kann, sind sogenannte Hardware-Sicherheitsmodule (HSM). Solche Geräte sind beispielsweise in der Finanzbranche üblich, werden aber auch beim besonderen elektronischen Anwaltspostfach eingesetzt. Im Normalbetrieb lassen HSM nur vorher definierte Anfragen zu; darüber hinaus gehende Daten werden nicht preisgegeben.[168] Es besteht somit auch ein Schutz gegen Innentäter; Angriffe auf die Hardware führen i.d.R. zur Zerstörung der Daten. So lassen sich Zugriffsbeschränkungen sicher umsetzen und die Rate von Anfragen limitieren. Soll, etwa wegen Hardware-Defekten, eine Übertragung des Inhalts eines HSM auf ein anderes erfolgen, ist ein über den Normalbetrieb hinausgehender Zugriff erforderlich. Dieser lässt sich an Bedingungen knüpfen – in der Regel die Verwendung mehrerer kryptographischer Schlüssel, die bei verschiedenen Personen hinterlegt sind. Hier könnten wiederum die Datenschutzaufsichtsbehörden in Spiel kommen.

Es sei an dieser Stelle betont, dass die Verwendung eines HSM alleine noch keine Sicherheit erzeugt; vielmehr muss auch ein HSM in eine Sicherheitsarchitektur eingebunden werden, die sowohl technische als auch organisatorische Maßnahmen umfasst.

6. Beschränkung des Verwendungszwecks

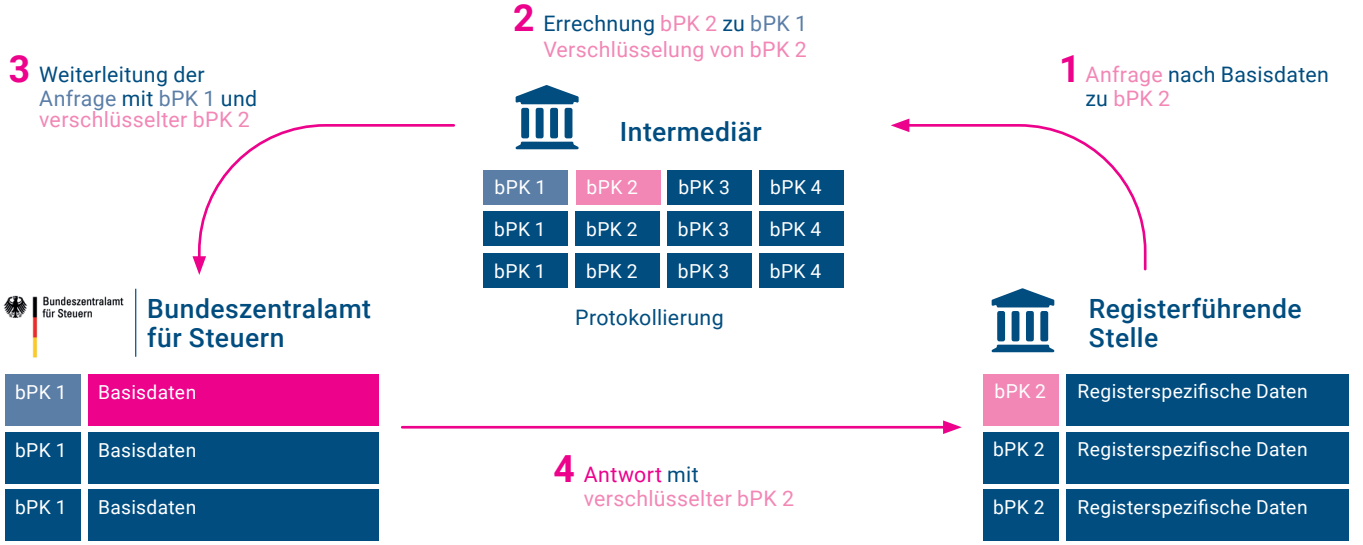
Es ist durchaus denkbar, die Zuordnung von bPK lediglich auf wenige, festgelegte Zwecke wie den Zensus zu beschränken. Die Abwägung zwischen den Vorteilen durch eine weitergehende Registerkonsolidierung und den Risiken für die Privatsphäre der Betroffenen soll an dieser Stelle nicht vertieft werden. Sie muss jedoch vom Gesetzgeber reflektiert werden.

[163] Vgl. § 7 Abs. 2, § 9 Abs. 1 IDNrG-E.
[164] Siehe oben unter B. III.
[165] Siehe oben unter B. IV. 2.
[166] Vgl. *Pauly in Paal/Pauly*, DSGVO, 2. Aufl. 2018, Art. 87 Rn. 3; *Ehmann* in *Ehmann/Selmayr*, DSGVO, Art. 87 Rn. 9.
[167] Siehe oben unter B. III. 3. c) (1).
[168] Ausführlich zur Funktionsweise von Hardware-Sicherheitsmodulen *Smith* in *Rosenberg* (Hrsg.) 2010, Handbook of Financial Cryptography and Security, 257ff.

ERGÄNZENDE INFORMATIONEN

Eine weitere Option besteht darin, einer Behörde aus einem Bereich die bPK eines anderen Bereichs verschlüsselt zugänglich zu machen – und zwar, wie mit asymmetrischer Kryptographie problemlos machbar, dass Behörden immer nur die für ihren eigenen Bereich gültige bPK entschlüsseln können. Somit ist neben den durch den Regierungsentwurf bereits vorgesehenen Abläufen auch eine direkte Kommunikation der Behörden untereinander machbar, wobei eine Behörde fremde bPK nie im Klartext zu sehen bekäme. Die vorgesehene Protokollierung von Datenabrufen, die der Transparenz gegenüber dem Bürger dient, müsste dann anhand der Abrufe der verschlüsselten bPK erfolgen oder dezentral durch die beteiligten Behörden angestoßen werden. Beispielhaft ist dieser Ablauf in **Abbildung 17** dargestellt.

Abb. 17 | Variante mit verschlüsselter Übermittlung von bPK



VI. Zwischenfazit

Wir möchten an dieser Stelle betonen, dass die hier entwickelten Modelle – einschließlich der dargestellten Ergänzungen des Grundmodells – nicht als Idealmodell einer IdentitätsmanagementInfrastruktur für die öffentliche Verwaltung in Deutschland angesehen werden sollten. Vielmehr sind diese Modelle bewusst so gestaltet, dass die bestehenden Register möglichst wenig angepasst werden müssen. Ausgangspunkt unserer Überlegungen ist der Regierungsentwurf, dessen grundsätzliche Architektur vorliegend übernommen und nur dort angepasst wird, wo wir Möglichkeiten sehen, Missbrauchspotentiale ohne Einschränkungen der Funktionalität zu reduzieren.

Abbildung 18 und **Abbildung 19** zeigen die wesentlichen Eigenschaften beider Modelle für bereichsspezifische Personenkennzeichen in einer zusammenfassenden Darstellung. Sie sehen die weitgehend zentrale Vergabe der bPK vor – im Stammzahl-Modell als Ableitung aus einer zufällig gewählten Stammzahl pro Betroffenem, bei NEU-ID direkt als Zufallszahl oder durch Übernahme bestehender bPK. Es ist grundsätzlich die Erfassung beliebiger Personengruppen möglich; wir gehen hier von natürlichen Personen (Deutschen und in Deutschland lebenden Ausländern) aus.

Beide Modelle ermöglichen den Zugriff auf einen Basisdatensatz, der wie im Regierungsentwurf vorgesehen beim Bundeszentralamt für Steuern gespeichert werden kann. Sie erzwingen ihn jedoch nicht. Das Stammzahl-Modell leitet bPK bei Bedarf aus Stammzahlen ab; im NEU-ID-Modell werden bPK beim Intermediär gespeichert. Während sonstige Aufgaben der Registermodernisierungsbehörde unberührt bleiben, favorisieren wir in beiden Modellen eine Wahrnehmung der Rolle zumindest des zentralen Intermediärs bei einer unabhängigen Stelle wie den Datenschutz-Aufsichtsbehörden. Dieses Vorgehen reduziert die Wahrscheinlichkeit eines Missbrauchs (wie die Herausgabe von bPK-Zuordnungen ohne Rechtsgrundlage) und reduziert schlimmstenfalls die Zahl der davon Betroffenen. Die Folgen möglicher Sicherheitsvorfälle können durch einen föderierten Ansatz (Verteilung von Intermediären bzw. Vermittlungsstellen) reduziert werden. Schränkt man die möglichen bPK-Zuordnungen so weit wie möglich ein und reduziert mit geeigneten technischorganisatorischen Maßnahmen – insbesondere auch durch sichere Hardware (HSM), die wir bei beiden Modellen favorisieren – die Erfolgswahrscheinlichkeit externer und interner Angreifer, so lässt sich bereits zeitnah ein akzeptables Datenschutzniveau erreichen. Die Umsetzung einer lokalen Intermediärsfunktion, die die Zuordnungen – und damit die Freigabe der dadurch zugreifbaren Daten – direkt beim Betroffenen vor-

nimmt, mag erst mittelfristig umgesetzt werden können. Sie kann die ansonsten vorgesehenen Intermediäre nicht ersetzen, aber in geeigneten Anwendungsfällen die Kontrolle des Bürgers über seine personenbezogenen Daten stärken.

Als Leitbild kann insgesamt gelten: Legitime Zuordnungen zwischen den bPK verschiedener Bereiche bleiben möglich, illegitime können zuverlässiger als nach dem Regierungsentwurf verhindert werden. Wir gehen davon aus, dass die meisten Aspekte des von uns vorgeschlagenen Modells sich bereits kurzfristig realisieren lassen. Unverzichtbar erscheint uns aber dessen Weiterentwicklung, insbesondere mit dem Ziel, den Betroffenen möglichst weitreichende Kontrolle über den Umgang mit ihren personenbezogenen Daten zu geben.

Es kann an dieser Stelle nicht deutlich genug betont werden, dass die Struktur der Register an sich durch die hier entwickelten Modelle nicht tangiert wird. Im Vergleich zum Regierungsentwurf ersetzt lediglich eine bPK die dort vorgesehene Steuer-ID. Wesentliche Änderungen betreffen nur den vorgesehenen Intermediär.

Abb. 18 | Morphologischer Kasten zum Identitätsnummernsystem Stammzahl-Modell

ID-NR-SYSTEM	AUSPRÄGUNGSFORMEN				
Typus von Personenkennzeichen	allgemeines Personenkennzeichen (aPK)	bereichsübergreifendes Personenkennzeichen (2wPK)	**bereichsspezifisches Personenkennzeichen (bPK)**		
Vorgehen bei der Vergabe	**Personenkennzeichen zentral vergeben**		Personenkennzeichen dezentral vergeben		
Inhaltliche Gestaltung des Personenkennzeichens	Steuer-ID	Andere existierende Register-ID	**Stammzahl als Zufallszahl generiert**	Keine zentrale ID	
Identifizierung in anderen Registern	Steuer-ID	Bisherige Register-ID	**Hashwert auf Stammzahl und Bereichs-Bezeichner**	Zufallszahl	
Zu erfassende Personengruppe	**Deutsche Bürger**	**Ausländer**	Steuerzahler	**Natürliche Personen**	Juristische Personen
Verortung der Speicherung der Basisdatensätze zu allen Personen	**Basisdatensatz beim Bundeszentralamt für Steuern (BZSt)**		ohne Basisdatensatz		
Einsatz einer Intermediär-internen Datenbank mit allen bPKs	**Verzicht auf Intermediär-interne ID-Datenbank**		Pseudonymisierte Intermediär-interne ID-Datenbank		
Registermodernisierung	**Registermodernisierungsbehörde (BVA)**		Verzicht auf Registermodernisierungsbehörde		
Verortung der Intermediäre zu den BZSt-Basisdatensätzen	Intermediär zum BZSt-Basisdatensatz bei BVA (Registermodernisierungsbehörde)		**Intermediär zum BZSt-Basisdatensatz bei Datenschutzaufsichtsbehörde**		
Vermittlungsstellen für Anfragen auf BZSt-Basisdatensätze	Keine Vermittlungsstelle für Anfragen	Zentrale Vermittlungsstelle für Anfragen	**Verbund von Vermittlungsstellen für Anfragen**		
Prüfung der Zugriffe auf BZSt-Basisdatensätze	Keinerlei Prüfung der Zugriffe	Software-basierte Prüfung der Zugriffe	**Hardware-basierte Prüfung der Zugriffe**	Ständige Prüfung durch Sachbearbeiter	
Freigabe von Daten durch Bürger bei bereichsübergreifenden Abfragen	Freigabe von Daten ohne Bürgereinbindung	**Anlassbezogene Freigabe von Daten durch Bürger**	Freigaben von Daten stets durch Bürger erforderlich		

Abb. 19 | Morphologischer Kasten zum Identitätsnummernsystem NEU-ID

ID-NR-SYSTEM	AUSPRÄGUNGSFORMEN			
Typus von Personenkennzeichen	allgemeines Personenkennzeichen (aPK)	bereichsübergreifendes Personenkennzeichen (2wPK)	**bereichsspezifisches Personenkennzeichen (bPK)**	
Vorgehen bei der Vergabe	**Personenkennzeichen zentral vergeben**	Personenkennzeichen dezentral vergeben		
Inhaltliche Gestaltung des Personenkennzeichens	Steuer-ID	Andere existierende Register-ID	**NEU-ID in Form von einer Zufallszahl**	Keine zentrale ID
Identifizierung in anderen Registern	Steuer-ID	**Bisherige Register-ID**	Hashwert auf Stammzahl und Bereichs-Bezeichner	**Zufallszahl**
Zu erfassende Personengruppe	**Deutsche Bürger**	**Ausländer**	Steuerzahler	**Natürliche Personen**	Juristische Personen
Verortung der Speicherung der Basisdatensätze zu allen Personen	**Basisdatensatz beim Bundeszentralamt für Steuern (BZSt)**	ohne Basisdatensatz		
Einsatz einer Intermediär-internen Datenbank mit allen bPKs	Verzicht auf Intermediär-interne ID-Datenbank	**Pseudonymisierte Intermediär-interne ID-Datenbank**		
Registermodernisierung	**Registermodernisierungsbehörde (BVA)**	Verzicht auf Registermodernisierungsbehörde		
Verortung der Intermediäre zu den BZSt-Basisdatensätzen	Intermediär zum BZSt-Basisdatensatz bei BVA (Registermodernisierungsbehörde)	**Intermediär zum BZSt-Basisdatensatz bei Datenschutzaufsichtsbehörde**		
Vermittlungsstellen für Anfragen auf BZSt-Basisdatensätze	Keine Vermittlungsstelle für Anfragen	Zentrale Vermittlungsstelle für Anfragen	**Verbund von Vermittlungs-stellen für Anfragen**	
Prüfung der Zugriffe auf BZSt-Basisdatensätze	Keinerlei Prüfung der Zugriffe	Software-basierte Prüfung der Zugriffe	**Hardware-basierte Prüfung der Zugriffe**	Ständige Prüfung durch Sachbearbeiter
Freigabe von Daten durch Bürger bei bereichs-übergreifenden Abfragen	Freigabe von Daten ohne Bürgereinbindung	**Anlassbezogene Freigabe von Daten durch Bürger**	Freigaben von Daten stets durch Bürger erforderlich	

E. Abschließende Bewertung und Empfehlung

Zielsetzung aller Beteiligten sollte es sein, das RegMoG auf einen verfassungsgemäßen Weg zu bringen.

Der vorliegende Gesetzesentwurf, der einen erheblichen Modernisierungsschub für die Bundesrepublik Deutschland und E-Government bringen soll, kann diesen hohen Erwartungen aus technischen wie rechtlichen Gründen nicht gerecht werden. Idealerweise würde der Entwurf die Grundlagen für ein leistungsfähiges, datenschutzkonformes, sicheres und vertrauenswürdiges Identitätsnummernsystem legen, um die in der Einführung des Gesetzesentwurf aufgezählten Probleme dauerhaft zu lösen. Im Falle einer Umsetzung bekommen die Bürger allerdings eine allgemeine Personenkennziffer und ein digitales Identitätsnummernsystem auf Basis der Steuer-ID. Künftige Regierungen oder die Europäische Union könnten dies rasch zu einem Profil- und Überwachungssystem über alle Bürger ausbauen. Diese Gefahr besteht nicht nur theoretisch. Mit Blick auf die Machtübernahmen in einigen mittlerweile autokratisch regierten Staaten ist sie ganz reell. Wir halten es für wichtig, auch diesen Aspekt bei der Gesetzgebung im Blick zu halten.

Dass mit dem vorliegenden Gesetzesentwurf die Steuer-ID zu einem allgemeinen Personenkennzeichen wird, erscheint – auch, wenn zunächst nicht alle Register eingebunden werden – unzweifelhaft. Wir sehen deshalb eine große Wahrscheinlichkeit, dass dieses Gesetz im Fall seines Inkrafttretens durch das Bundesverfassungsgericht für nichtig erklärt werden wird.

Ursprünglich sollte das Gesetz mit Verweis auf Kosten- und Zeitargumente vor der Weihnachtspause durch den Bundestag und den Bundesrat gehen. Gelänge dies, würde in einigen Monaten ein vollkommener Neustart des Vorhabens drohen. Dies hätte erhebliche Verzögerungen und zusätzliche unnötige Kosten zur Folge. An diesen hat zu diesem Zeitpunkt keiner der Beteiligten ein Interesse, weder die Bundesregierung noch die Datenschutzbeauftragten und auch nicht die Bürger. Das reale Risiko von vielen Verfassungsbeschwerden, die im Vorfeld und bei der ersten Lesung im Deutschen Bundestag bereits angekündigt wurden, muss bei der weiteren Abwägung berücksichtigt werden.

Insofern wären die Bundesregierung und der IT-Planungsrat gut beraten, sich trotz des laufenden Gesetzgebungsverfahren bereits mit Alternativen auseinanderzusetzen und diese so vorzubereiten, dass im Falle eines Scheiterns ein überzeugender Alternativplan ausgearbeitet vorliegt und nicht noch weitere wertvolle Zeit verloren geht.

Mit Blick auf die Optionen und vorhandenen Alternativen zu Personenkennzeichen und Identitätsnummernsystemen gilt festzuhalten, dass der Vorschlag des RegMoG der Bundesregierung keineswegs alternativlos ist. Allerdings muss auch der Wille vorhanden sein, den eingeschlagenen Pfad zu verlassen, sollte sich dieser als für die Sache ungeeignet erweisen.

Das Gutachten zeigt auf, dass es jenseits der Steuer-ID als Identitätsnummer weitere Optionen für Personenkennzeichen und Identitätsnummernsysteme gibt. Diese können zeitnah untersucht, bewertet und bei Bedarf professionell umgesetzt werden. Dazu müsste die Analyse und Konzeption verschiedener Lösungsmodelle für ein Identitätsmanagement noch einmal geöffnet und eine nachhaltige Lösung gefunden werden.

Wir haben mit diesem Gutachten zwei Varianten vorgestellt, die aus unserer Sicht beide eine substantielle Verbesserung gegenüber dem Vorschlag der Bundesregierung bedeuten.[169] Ohne Risiko sind auch diese Ansätze nicht, denn wenn Daten für legitime Zwecke wie die Registerkonsolidierung zusammengeführt werden können, ist dies im Grundsatz auch immer für illegitime Zwecke möglich. Die Ansätze reduzieren die Risiken für den Datenschutz jedoch, indem sie eine Umgehung der schon im Regierungsentwurf vorgesehenen Intermediäre erschweren. Gleichzeitig können sie ohne nennenswerte Eingriffe in die bestehende Registerstruktur realisiert werden. Sollte sich eine dieser beiden Optionen oder ein anderer Ansatz als zielführender erweisen, wären die Bundesregierung und der IT-Planungsrat in der Lage, binnen weniger Monate einen überzeugenderen, professionelleren Ansatz in ein neues Gesetzgebungsverfahren einzubringen und diesen zeitnah umzusetzen.

Zugegeben würde dies zu einem Ende des laufenden Gesetzgebungsverfahrens führen. Die noch erforderlichen strukturellen Überarbeitungen am Entwurf wären aber zu einschneidend, als dass der Gesetzgeber diesen durch Anpassungen noch retten könne. Der bisherige Erkenntnisgewinn im Diskurs um die beste Lösung war jedoch hoch und lohnenswert. Insofern kann es auf dem bestehenden Erkenntnisniveau mit einer besseren Lösung rasch in einem weiteren Gesetzgebungsverfahren weitergehen.

Unabhängig vom Ausgang der Debatte im Ausschuss handelt es sich bei dem RegMoG um ein Gesetz mit erheblichen Folgen für alle Bürger und Einwohner der Bundesrepublik Deutschland. Hierbei gibt es unterschiedliche und politisch sehr umstrittene Positionen quer durch alle Parteien und öffentliche Institutionen. Politisch ist das legitim, aber für den Staat und das hohe Vertrauen seiner Bürger in Bund, Länder und Kommunen auch riskant.

[169] Vgl. für eine zusammenfassende Darstellung Abschnitt D.VI

Literatur

Article 29 Data Protection Working Party, Opinion on Purpose Limitation, 2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Brink, Stefan/Wolff, Heinrich Amadeus (Hrsg.), Beck'scher Onlinekommentar, 23. Edition 2020 (zitiert als *Bearbeiter*, in: BeckOK)

Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, Part 2, Version 2.21, 2016, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-2-V2_2.pdf?__blob=publicationFile&v=3, (zitiert als BSI TR 03110 Part 2)

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI), BfDI, Hintergrundpapier zur Registermodernisierung und Schaffung eines einheitlichen Personenkennzeichens, 2020, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Hintergrundpapier-Registermodernisierung.html

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI), 23. Tätigkeitsbericht zum Datenschutz 2009 und 2010, 2010, https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/23TB_09_10.pdf?__blob=publicationFile&v=9

Bundesbeauftragter für den Datenschutz, Tätigkeitsbericht zum Datenschutz 2003 und 2004, 2004, https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/20TB_03_04.html

Bundesrat, Empfehlungen der Ausschüsse zum Entwurf eines Gesetzes zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (RegMoG), Drucksache 563/1/20

Bundesvereinigung Deutscher Arbeitgeberverbände (BDA), Einführung einer Identifikationsnummer ist wichtig, aber noch nicht ausreichend. Stellungnahme zum Referentenentwurf des BMI zum Registermodernisierungsgesetz, 2020, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/registermodernisierungsgesetz/bda.pdf?__blob=publicationFile&v=1

Bundesrechtsanwaltskammer (BRAK), Stellungnahme, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/registermodernisierungsgesetz/bundesrechtsanwaltskammer.pdf?__blob=publicationFile&v=3

Databund, Stellungnahme zum Registermodernisierungsgesetz, 2020, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/registermodernisierungsgesetz/databund.pdf?__blob=publicationFile&v=3

Datenethikkommission der Bundesregierung, Gutachten, 2019, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6

Deutscher Anwaltverein (DAV), Stellungnahme, 2020, https://anwaltverein.de/de/newsroom/sn-75-20-zum-registermodernisierungsgesetz

Deutsche Rentenversicherung (DRV), Stellungnahme, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/registermodernisierungsgesetz/rentenversicherung.pdf?__blob=publicationFile&v=2

Ehmann, Eugen/Selmayr, Martin (Hrsg.), DSGVO. Kommentar, 2. Auflage München 2018 (zitiert als *Bearbeiter*, in: Ehmann/Selmayr)

Gola, Peter (Hrsg.), DSGVO, 2. Auflage, München 2018 (zitiert als: *Bearbeiter* in: Gola)

Gesellschaft für Informatik, Stellungnahme des Fachbereichs Informatik in Recht und Öffentlicher Verwaltung und des Präsidiums-Arbeitskreises Datenschutz und IT-Sicherheit der Gesellschaft für Informatik e.V. (GI)zum Referentenentwurf eines Gesetzes zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz–RegMoG) des Bundesministeriums des Innern, für Bau und Heimat (BMI), 2020, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/registermodernisierungsgesetz/gfi.pdf?__blob=publicationFile&v=3

Hornung, Gerrit, Die digitale Identität, Baden-Baden 2005

Humanistische Union (HU), Stellungnahme der Humanistischen Union zum Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat: Entwurf eines Gesetzes zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz – RegMoG), 2020, http://www.humanistische-union.de/typo3/ext/naw_securedl/secure.php?u=0&file=uploads/media/2020-09-04_HUStN_Registermodernisierungsgesetz.pdf&t=1599569825&hash=932c9fa5b37c6dd7f8fcf46228653b3e

IT-Planungsrat 2020: Eckpunkte für die Registermodernisierung – Bestehende Anforderungen, vorläufige Architekturskizze sowie sich daraus ergebende Maßnahmen im Rahmen des IT-Planungsratsprojekts Registermodernisierung, 2020, https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/32_Sitzung/TOP_06_Anlage_1_Eckpunkte.pdf?__blob=publicationFile&v=3

Katz, Jonathan/Lindell, Yehuda, Introduction to Modern Cryptography, 2. Auflage, London 2014

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), Entschließung Registermodernisierung verfassungskonform umsetzen, 2020, https://www.datenschutzkonferenz-online.de/media/en/20200828_entschlie%C3%9Fung_pkz_final_1.pdf

Körner, Thomas/Krause, Anja/Ramsauer, Katharina, Anforderungen und Perspektiven auf dem Weg zu einem künftigen Registerzensus, in: WISTA – Wirtschaft und Statistik, Sonderheft Zensus 2021, Statistisches Bundesamt, Wiesbaden 2019, https://www.destatis.de/DE/Methoden/WISTA-Wirtschaft-und-Statistik/2019/07/anforderungen-perspektiven-registerzensus-072019.pdf?__blob=publicationFile

Kühling, Jürgen/Buchner, Benedikt, DSGVO und BDSG. Kommentar, 3. Auflage München 2020 (zitiert als *Bearbeiter*, in: Kühling/Buchner)

Martini, Mario/Wagner, David/Wenzel, Michael, Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, 2017, https://www.normenkontrollrat.bund.de/resource/blob/72494/476034/eebab686008cfec0a7919ca03e51abe3/2017-10-06-download-nkr-gutachten-2017-anlage-untersuchung-datenschutz-data.pdf?download=1

Martini, Mario/Wenzel, Michael, »Once only« versus »only once«: Das Prinzip einmaliger Erfassung zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit, DVBl. 2017, S. 749 ff.

Maunz-Dürig, Grundgesetz Kommentar, 91. Auflage, München 2020 (zitiert als: *Bearbeiter*, in: Maunz-Dürig)

Nationaler Normenkontrollrat, Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren, 2017, https://www.normenkontrollrat.bund.de/resource/blob/300864/476004/12c91fffb877685f4771f34b9a5e08fd/2017-10-06-download-nkr-gutachten-2017-data.pdf

Nationaler Normenkontrollrat und McKinsey & Co, Ergänzende Dokumentation zu „Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren.", Nationaler Normenkontrollrat, Berlin 2017, https://www.normenkontrollrat.bund.de/resource/blob/72494/476010/b6c476acd8bac8d1a81c1f7b7212cabd/2017-10-06-download-nkr-gutachten-2017-anlage-dokumentation-data.pdf?download=1.

Paal, Boris/Pauly, Daniel A. (Hrsg.), DSGVO und DSG. Kommentar. 2. Auflage, München 2019

Roßnagel, Alexander, Kontinuität oder Innovation? Der deutsche Spielraum in der Anpassung des bereichsspezifischen Datenschutzrechts, DuD 2018, S. 477 ff.

Schaar, Peter, Steuer-ID darf kein allgemeines Personenkennzeichen werden!, ZD 2011, 49 f.

Simitis, Spiros/Hornung, Gerrit/Spiecker genannt Döhmann, Indra (Hrsg.), Datenschutzrecht. Kommentar, Baden-Baden, 2019 (zitiert als *Bearbeiter*, in: Simitis/Hornung/Spiecker gen. Döhmann)

Smith, Sean, Hardware Security Modules, in Rosenberg, Burton (Hrsg.), Handbook of Financial Cryptography and Security, London 2010, S. 257 ff.

Sorge, Christoph/Leicht, Maximilian, Registermodernisierungsgesetz – eine datenschutzgerechte Lösung?, ZRP 2020, S. 242 ff.

Stallings, William, Cryptography and Network Security, 7. Auflage, Pearson India 2017

Statistisches Bundesamt, Ein Blick in die Registerlandschaft in Deutschland. Beistellung zum Gutachten „Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren." im Auftrag des Nationalen Normenkontrollrates, 2017, https://www.normenkontrollrat.bund.de/resource/blob/72494/476024/04a6019c945895d3587136ff2ce46b73/2017-10-06-download-nkr-gutachten-2017-anlage-untersuchung-staba-register-data.pdf?download=1

Stocksmeier, Dirk/Hunnius, Sirko, OZG-Umsetzungskatalog – Digitale Verwaltungsleistungen im Sinne des Onlinezugangsgesetzes,]init[AG, Berlin 2018, https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/26_Sitzung/TOP2_Anlage_OZGUmsetzungskatalog.pdf?__blob=publicationFile&v=4.

Voßkuhle, Andreas, Grundwissen Öffentliches Recht: Der Grundsatz des Vorbehalts des Gesetzes, Juristische Schulung (JuS) 2001, S. 118 f.

Wissenschaftlicher Dienst des Bundestages, Einführung einer registerübergreifenden einheitlichen Identifikationsnummer nach dem Entwurf eines RegistermodernisierungsgesetzesDSGVO und Recht auf informationelle Selbstbestimmung, 2020 https://cdn.netzpolitik.org/wp-upload/2020/09/WD-Registermodernisierung.pdf (zitiert als Wiss. Dienst BTag)

Über die Autoren

Prof. Dr.-Ing. Christoph Sorge

war nach seinem Studium der Informationswirtschaft und seiner Promotion in Informatik am KIT zunächst als Research Scientist bei den NEC Laboratories Europe tätig. Von 2010 bis 2014 war er Juniorprofessor für Sicherheit in Netzwerken an der Universität Paderborn. Anschließend wechselte er an die rechtswissenschaftliche Fakultät der Universität des Saarlandes, wo er Inhaber des Lehrstuhls für Rechtsinformatik ist. Gleichzeitig ist er als kooptierter Professor Mitglied der Fachrichtung Informatik der Universität, assoziiert mit dem CISPA Helmholtz-Zentrum für Informationssicherheit sowie Senior Fellow des Deutschen Forschungsinstituts für öffentliche Verwaltung Speyer. Mit seinem interdisziplinären Team forscht er an der Schnittstelle von Informatik und Recht, insbesondere im Bereich des Datenschutzes.

Prof. Dr. rer. publ. Jörn von Lucke

hat den Lehrstuhl für Verwaltungs- und Wirtschaftsinformatik am The Open Government Institute (TOGI) an der Zeppelin Universität Friedrichshafen inne. Seine aktuellen Forschungsschwerpunkte liegen in E-Government (Hochleistungsportale), Open Government (offenes Regierungs- und Verwaltungshandeln), offenen Daten, offener gesellschaftlicher Innovation, Smart Government (Internet der Dinge und Internet der Dienste im öffentlichen Sektor; Verwaltung 4.0, Smarte Stadt), Realtime Government und Künstlicher Intelligenz im öffentlichen Sektor. Zugleich vertritt er die Interessen der Gesellschaft für Informatik e.V. im Rahmen der deutschen Aktivitäten zur Open Government Partnership.

Prof. Dr. iur. Indra Spiecker
gen. Döhmann

hat Rechtswissenschaften in Bonn, Mainz und Washington studiert und war wissenschaftliche Mitarbeiterin an den Universitäten Bonn und Heidelberg sowie am Max-Planck-Institut für Gemeinschaftsgüter, Bonn. Von 2008 bis 2013 war sie Professorin für öffentliches Recht, Telekommunikationsrecht und Datenschutzrecht am Institut für Informations- und Wirtschaftsrecht des Karlsruher Instituts für Technologie. Seit 2013 ist sie Professorin für öffentliches Recht, Informationsrecht, Umweltrecht und Verwaltungswissenschaften an der Goethe-Universität Frankfurt. Dort ist sie auch Direktorin der Forschungsstelle Datenschutz. Sie wurde als erste Juristin in die Akademie der Technikwissenschaften (acatech) aufgenommen. Indra Spiecker ist Herausgeberin des Kommentars zum Datenschutzrecht (Simitis/Hornung/Spiecker genannt Döhmann).